



J.W. Price, 949/261,8433

Yuichi Futa

S.N. 09/603,636

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

NAK1-BLS3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 5月12日

出 願 番 号

Application Number:

特願2000-140886

出 願 人

Applicant (s):

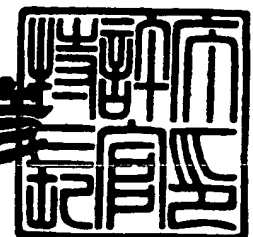
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月29日

特 許 庁 長 官
Commissioner,
Patent Office

近 藤 隆 彦



【書類名】 特許願

【整理番号】 2022520178

【提出日】 平成12年 5月12日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【選任した代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第203055号

【出願日】 平成11年 7月16日

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9810105

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 有限体上の連立方程式求解装置及び逆元演算装置

【特許請求の範囲】

【請求項 1】 有限体 $GF(p)$ (p は素数) 上の n 元連立一次方程式 $Ax = b$ (n は正の整数、 A は n 行 n 列の成分からなる係数行列、 x は n 個の成分からなる変数ベクトル、 b は n 個の成分からなる定数ベクトル) の解を求める連立方程式求解装置であって、

係数行列 A と定数ベクトル b とを記憶しているパラメタ記憶手段と、

前記パラメタ記憶手段から係数行列 A と定数ベクトル b とを読み出し、読み出した係数行列 A 及び定数ベクトル b を三角化変換して方程式 $Ax = b$ と同値の関係を有する n 元連立一次方程式 $Cx = d$ の係数行列 C (C は n 行 n 列の成分からなる係数行列) 及び定数ベクトル d (d は n 個の成分からなる定数ベクトル) を生成する三角化変換手段と、

前記三角化変換は、係数行列 A の各対角成分を 1 に変換しない、係数行列 A の上三角行列への変換であり、

生成された係数行列 C の各対角成分の有限体 $GF(p)$ 上の逆元である対角逆元を生成する対角逆元演算手段と、

生成された係数行列 C と定数ベクトル d と生成された各対角逆元とを用いて、方程式 $Ax = b$ の解として、方程式 $Cx = d$ の解を求める方程式求解手段とを備えることを特徴とする連立方程式求解装置。

【請求項 2】 前記三角化変換手段は、連続する 1 個以上の変換過程を介して前記方程式 $Cx = d$ の係数行列 C 及び定数ベクトル d を生成し、

前記各変換過程において、前記三角化変換手段は、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Ax = b$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $Cx = d$ であり、

前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象となる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方

程式である軸方程式とを含み、

前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第 1 係数群と第 2 係数群とを定め、

ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られ、

前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし

前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く

ことを特徴とする請求項 1 に記載の連立方程式求解装置。

【請求項 3】 前記三角化変換手段は、前記各変換過程において、1 個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換手段は、各副変換過程において、

軸方程式の 0 でない係数を有する最高次の変数の係数から構成される群を第 1 係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の 0 でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第 2 係数群と定め、

前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし

前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く

ことを特徴とする請求項 2 に記載の連立方程式求解装置。

【請求項 4】 前記三角化変換手段は、前記各変換過程において、1 個の係数

群算出過程と、前記係数群算出過程後に 1 個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換手段は、軸方程式及び 1 個以上の対象方程式の 0 でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる 2 個以上の値から構成される群を第 1 係数群と定め、

前記第 1 係数群に含まれる値であって、軸方程式の 0 でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた 1 個以上の値から構成される群を第 2 係数群と定め、

前記副変換過程において、前記三角化変換手段は、

前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし

前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く

ことを特徴とする請求項 2 に記載の連立方程式求解装置。

【請求項 5】 係数行列 C の対角成分を m_i ($i = 1, 2, \dots, n$) とし、対角成分 m_i の $GF(p)$ 上の対角逆元を I_i ($i = 1, 2, \dots, n$) とし、

前記対角逆元演算手段は、

【数 1】

$$t_i = \prod_{k=1}^n m_k \quad (m_i \text{ を除く}) \bmod p$$

$$(i = 1, 2, \dots, n)$$

を算出し、

【数 2】

$$t = \prod_{k=1}^n m_k \bmod p$$

を算出する乗算部と、

$$u = 1 / t \bmod p$$

を算出する第 1 逆元演算部と、

$$\text{対角逆元 } I_i = u \times t_i \bmod p \quad (i = 1, 2, \dots, n)$$

を算出する第 2 逆元演算部と

を含むことを特徴とする請求項 3～4 のいずれかに記載の連立方程式求解装置

【請求項 6】 前記乗算部は、

$$s_1 = m_1 \times m_2 \bmod p,$$

$$s_2 = s_1 \times m_3 \bmod p,$$

...

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

をこの順序で算出し、

次に、

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$$

$$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$$

$$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$$

...

$$s_5 = m_4 \times s_6 \bmod p$$

$$t_3 = s_1 \times s_5 \mod p$$

$$s_4 = m_3 \times s_5 \mod p$$

$$t_2 = m_1 \times s_4 \mod p$$

$$t_1 = m_2 \times s_4 \mod p$$

をこの順序で算出し、

次に、正の整数の集合 $\{1, 2, \dots, n\}$ から選択された 1 個の値 j について、

$$t = t_j \times m_j$$

を算出する

ことを特徴とする請求項 5 に記載の連立方程式求解装置。

【請求項 7】 有限体 $GF(p)$ (p は素数) の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数) の元 x の逆元 I を演算する逆元演算装置であって、

元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay = B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、

請求項 1 ～ 6 のいずれかに記載の連立方程式求解装置であって、 n 元連立一次方程式 $Ay = B$ の解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備えることを特徴とする逆元演算装置。

【請求項 8】 有限体 $GF(p)$ (p は素数) の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数) の上の楕円曲線を E 、楕円曲線 E のベースポイントを G とし、楕円曲線 E 上の離散対数問題を安全性の根拠として利用して安全性を確保する通信を行い、安全性の確保に際して拡大体 $GF(q)$ 上の元 x の逆元 I を算出する通信システムであって、

元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay = B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、

請求項 1 ～ 6 のいずれかに記載の連立方程式求解装置であって、 n 元連立一次方程式 $Ay = B$ の解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備えることを特徴とする通信システム。

【請求項9】 有限体 $GF(p)$ (p は素数)の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数)の上の楕円曲線を E 、楕円曲線 E のベースポイントを G とし、楕円曲線 E 上の離散対数問題を安全性の根拠として暗号化されたデジタル著作物を記録している記録媒体から暗号化デジタル著作物を読み出して復号し、復号に際して拡大体 $GF(q)$ 上の元 x の逆元 I を算出する記録媒体再生装置であって

元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay = B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、

請求項1～6のいずれかに記載の連立方程式求解装置であって、 n 元連立一次方程式 $Ay = B$ の解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備えることを特徴とする記録媒体再生装置。

【請求項10】 有限体 $GF(p)$ (p は素数)上の n 元連立一次方程式 $Ax = b$ (n は正の整数、 A は n 行 n 列の成分からなる係数行列、 x は n 個の成分からなる変数ベクトル、 b は n 個の成分からなる定数ベクトル)の解を求め、係数行列 A と定数ベクトル b とを記憶しているパラメタ記憶手段を備える連立方程式求解装置において用いられる連立方程式求解方法であって、

前記パラメタ記憶手段から係数行列 A と定数ベクトル b とを読み出し、読み出した係数行列 A 及び定数ベクトル b を三角化変換して方程式 $Ax = b$ と同値の関係を有する n 元連立一次方程式 $Cx = d$ の係数行列 C (C は n 行 n 列の成分からなる係数行列)及び定数ベクトル d (d は n 個の成分からなる定数ベクトル)を生成する三角化変換ステップと、

前記三角化変換は、係数行列 A の各対角成分を1に変換しない、係数行列 A の上三角行列への変換であり、

生成された係数行列 C の各対角成分の有限体 $GF(p)$ 上の逆元である対角逆元を生成する対角逆元演算ステップと、

生成された係数行列 C と定数ベクトル d と生成された各対角逆元とを用いて、方程式 $Ax = b$ の解として、方程式 $Cx = d$ の解を求める方程式求解ステップとを含むことを特徴とする連立方程式求解方法。

【請求項 11】 前記三角化変換ステップは、連続する 1 個以上の変換過程を介して前記方程式 $Cx = d$ の係数行列 C 及び定数ベクトル d を生成し、

前記各変換過程において、前記三角化変換ステップは、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Ax = b$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $Cx = d$ であり、

前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象となる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方程式である軸方程式とを含み、

前記三角化変換ステップは、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第 1 係数群と第 2 係数群とを定め、

ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られ、

前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし

前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く

ことを特徴とする請求項 10 に記載の連立方程式求解方法。

【請求項 12】 前記三角化変換ステップは、前記各変換過程において、1 個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換ステップは、各副変換過程において、

軸方程式の 0 でない係数を有する最高次の変数の係数から構成される群を第 1 係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の0でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第2係数群と定め、前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし

前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く

ことを特徴とする請求項11に記載の連立方程式求解方法。

【請求項13】 前記三角化変換ステップは、前記各変換過程において、1個の係数群算出過程と、前記係数群算出過程後に1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換ステップは、軸方程式及び1個以上の対象方程式の0でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる2個以上の値から構成される群を第1係数群と定め、

前記第1係数群に含まれる値であって、軸方程式の0でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた1個以上の値から構成される群を第2係数群と定め、

前記副変換過程において、前記三角化変換ステップは、

前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし

前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く

ことを特徴とする請求項11に記載の連立方程式求解方法。

【請求項14】 係数行列Cの対角成分を m_i ($i = 1, 2, \dots, n$)とし、対角成分 m_i のGF(p)上の対角逆元を I_i ($i = 1, 2, \dots, n$)とし、

前記対角逆元演算ステップは、

【数 3】

$$t_i = \prod_{k=1}^n m_k \quad (m_i \text{ を除く}) \bmod p$$

$$(i = 1, 2, \dots, n)$$

を算出し、

【数 4】

$$t = \prod_{k=1}^n m_k \bmod p$$

を算出する乗算部と、

$$u = 1 / t \bmod p$$

を算出する第 1 逆元演算部と、

$$\text{対角逆元 } I_i = u \times t_i \bmod p \quad (i = 1, 2, \dots, n)$$

を算出する第 2 逆元演算部と

を含むことを特徴とする請求項 12～13 のいずれかに記載の連立方程式求解方法。

【請求項 15】 前記乗算部は、

$$s_1 = m_1 \times m_2 \bmod p、$$

$$s_2 = s_1 \times m_3 \bmod p、$$

...

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

をこの順序で算出し、

次に、

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$\begin{aligned}
 t_{n-1} &= s_{n-3} \times m_n \mod p \\
 s_n &= m_{n-1} \times m_n \mod p \\
 t_{n-2} &= s_{n-4} \times s_n \mod p \\
 s_{n-1} &= m_{n-2} \times s_n \mod p \\
 t_{n-3} &= s_{n-5} \times s_{n-1} \mod p \\
 s_{n-2} &= m_{n-3} \times s_{n-1} \mod p \\
 t_{n-4} &= s_{n-6} \times s_{n-2} \mod p \\
 &\dots
 \end{aligned}$$

$$\begin{aligned}
 s_5 &= m_4 \times s_6 \mod p \\
 t_3 &= s_1 \times s_5 \mod p \\
 s_4 &= m_3 \times s_5 \mod p \\
 t_2 &= m_1 \times s_4 \mod p \\
 t_1 &= m_2 \times s_4 \mod p
 \end{aligned}$$

をこの順序で算出し、

次に、正の整数の集合 $\{1, 2, \dots, n\}$ から選択された1個の値 j について、

$$t = t_j \times m_j$$

を算出する

ことを特徴とする請求項14に記載の連立方程式求解方法。

【請求項16】 有限体 $GF(p)$ (p は素数) 上の n 元連立一次方程式 $Ax = b$ (n は正の整数、 A は n 行 n 列の成分からなる係数行列、 x は n 個の成分からなる変数ベクトル、 b は n 個の成分からなる定数ベクトル) の解を求め、係数行列 A と定数ベクトル b とを記憶しているパラメタ記憶手段を備えるコンピュータで用いられる連立方程式求解プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記プログラムは、

前記パラメタ記憶手段から係数行列 A と定数ベクトル b とを読み出し、読み出した係数行列 A 及び定数ベクトル b を三角化変換して方程式 $Ax = b$ と同値の関係を有する n 元連立一次方程式 $Cx = d$ の係数行列 C (C は n 行 n 列の成分から

なる係数行列) 及び定数ベクトル d (d は n 個の成分からなる定数ベクトル) を生成する三角化変換ステップと、

前記三角化変換は、係数行列 A の各対角成分を 1 に変換しない、係数行列 A の上三角行列への変換であり、

生成された係数行列 C の各対角成分の有限体 $GF(p)$ 上の逆元である対角逆元を生成する対角逆元演算ステップと、

生成された係数行列 C と定数ベクトル d と生成された各対角逆元とを用いて、方程式 $Ax = b$ の解として、方程式 $Cx = d$ の解を求める方程式求解ステップとを含むことを特徴とする記録媒体。

【請求項 17】 前記三角化変換ステップは、連続する 1 個以上の変換過程を介して前記方程式 $Cx = d$ の係数行列 C 及び定数ベクトル d を生成し、

前記各変換過程において、前記三角化変換ステップは、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Ax = b$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $Cx = d$ であり、

前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象となる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方程式である軸方程式とを含み、

前記三角化変換ステップは、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第 1 係数群と第 2 係数群とを定め、

ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られ、

前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし

前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く

ことを特徴とする請求項17に記載の記録媒体。

【請求項18】 前記三角化変換ステップは、前記各変換過程において、1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換ステップは、各副変換過程において、

軸方程式の0でない係数を有する最高次の変数の係数から構成される群を第1係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の0でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第2係数群と定め、

前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし

前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く

ことを特徴とする請求項17に記載の記録媒体。

【請求項19】 前記三角化変換ステップは、前記各変換過程において、1個の係数群算出過程と、前記係数群算出過程後に1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換ステップは、軸方程式及び1個以上の対象方程式の0でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる2個以上の値から構成される群を第1係数群と定め、

前記第1係数群に含まれる値であって、軸方程式の0でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた1個以上の値から構成される群を第2係数群と定め、

前記副変換過程において、前記三角化変換ステップは、

前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし

前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く

ことを特徴とする請求項17に記載の記録媒体。

【請求項20】 係数行列Cの対角成分を m_i ($i=1, 2, \dots, n$)とし、対角成分 m_i のGF(p)上の対角逆元を I_i ($i=1, 2, \dots, n$)とし、

前記対角逆元演算ステップは、

【数5】

$$t_i = \prod_{k=1}^n m_k \text{ (} m_i \text{ を除く) mod } p$$

$$(i=1, 2, \dots, n)$$

を算出し、

【数6】

$$t = \prod_{k=1}^n m_k \text{ mod } p$$

を算出する乗算部と、

$$u = 1 / t \text{ mod } p$$

を算出する第1逆元演算部と、

$$\text{対角逆元 } I_i = u \times t_i \text{ mod } p \quad (i=1, 2, \dots, n)$$

を算出する第2逆元演算部と

を含むことを特徴とする請求項18～19のいずれかに記載の記録媒体。

【請求項21】 前記乗算部は、

$$s_1 = m_1 \times m_2 \mod p,$$

$$s_2 = s_1 \times m_3 \mod p,$$

...

$$s_{n-3} = s_{n-4} \times m_{n-2} \mod p$$

をこの順序で算出し、

次に、

$$t_n = s_{n-3} \times m_{n-1} \mod p$$

$$t_{n-1} = s_{n-3} \times m_n \mod p$$

$$s_n = m_{n-1} \times m_n \mod p$$

$$t_{n-2} = s_{n-4} \times s_n \mod p$$

$$s_{n-1} = m_{n-2} \times s_n \mod p$$

$$t_{n-3} = s_{n-5} \times s_{n-1} \mod p$$

$$s_{n-2} = m_{n-3} \times s_{n-1} \mod p$$

$$t_{n-4} = s_{n-6} \times s_{n-2} \mod p$$

...

$$s_5 = m_4 \times s_6 \mod p$$

$$t_3 = s_1 \times s_5 \mod p$$

$$s_4 = m_3 \times s_5 \mod p$$

$$t_2 = m_1 \times s_4 \mod p$$

$$t_1 = m_2 \times s_4 \mod p$$

をこの順序で算出し、

次に、正の整数の集合 {1, 2, ..., n} から選択された1個の値jについて、

$$t = t_j \times m_j$$

を算出する

ことを特徴とする請求項20に記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術及び誤り訂正技術に関し、特に、拡大体及び連立方程式を用いる演算技術に関する。

【0002】

【従来の技術】

近年、秘密通信方式やデジタル署名方式による通信が用いられるようになって
いる。

秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号方式と呼ばれる暗号方式を用いる。公開鍵暗号方式は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。

【0003】

公開鍵暗号方式では、暗号化鍵と復号化鍵とが異なり、復号化鍵を秘密にし、暗号化鍵を公開する。この公開鍵暗号方式の安全性の根拠として離散対数問題が用いられる。離散対数問題には代表的なものとして、有限体上定義されるもの及び楕円曲線上定義されるものがある。離散対数問題については、「A Course in Number theory and Cryptography」(Neal Koblitz著、Springer-Verlag,1987)に詳しく述べられている。

(楕円曲線上の離散対数問題)

楕円曲線上の離散対数問題とは、

E を有限体 $GF(q)$ ($q = p^n$ 、 p は素数、 n は正の整数) 上定義された楕円曲線とし、楕円曲線 E の位数が大きな素数で割り切れるとき、楕円曲線 E 上の元 G をベースポイントとする。このとき、楕円曲線 E 上の与えられた元 Y に対して、

$$Y = x * G$$

となる整数 x が存在するならば、 x を求めよ、という問題である。

【0004】

なお、この明細書において、演算子 $*$ は、楕円曲線上の加算を意味し、 $x * G$

は、楕円曲線上で G を x 回加算することを示す。また、 $GF(q)$ は $GF(p)$ の拡大体である。拡大体については、「現代暗号」（岡本龍明、山本博資著、シリーズ／情報科学の数学、産業図書、1997、26～28ページ）に詳しく述べられている。

（従来例1：楕円曲線上の離散対数問題を応用するエルガマル署名）

次に、楕円曲線上の離散対数問題を応用するエルガマル署名について、図9に示すシーケンス図を用いて説明する。

【0005】

ユーザAが使用する装置（以下、ユーザA310と称する。）、管理センタにおいて使用される装置（以下、管理センタ320と称する。）及びユーザBが使用する装置（以下、ユーザB330と称する。）は、それぞれネットワークで接続されている。

p を素数、 $q = p^n$ 、 n は正の整数、有限体 $GF(q)$ 上の楕円曲線を E とする。楕円曲線 E のベースポイントを G とし、 G の位数を r とする。すなわち、 r は、

$$r * G = 0$$

を満たす最小の正整数である。ここで、 0 は楕円曲線の群の加算における零元である。

【0006】

（1）管理センタ320による公開鍵の生成

管理センタ320は、ユーザA310からユーザA310が秘密に所有する秘密鍵 x_A を予め通知されており（ステップS1）、秘密鍵 x_A を用いて、次の式より、ユーザA310の公開鍵 Y_A を作成する（ステップS2）。

$$Y_A = x_A * G$$

その後、管理センタ320は、有限体 $GF(q)$ 、楕円曲線 E 及びベースポイント G をシステムパラメータとして公開し、ユーザB330にユーザA310の公開鍵 Y_A を公開する（ステップS3～S4）。

【0007】

（2）ユーザA310による署名生成

ユーザ A310 は、乱数 k を生成する (ステップ S5)。次に、ユーザ A310 は、

$$R_1 = (r_x, r_y) = k * G$$

を計算し (ステップ S6)、

$$s * k = m + r_x \times x_A \mod r$$

から、 s を計算する (ステップ S7)。ここで、 m は、ユーザ A310 がユーザ B330 へ送信するメッセージである。

【0008】

さらに、ユーザ A310 は、得られた (R_1, s) を署名としてメッセージ m とともに、ユーザ B330 へ送信する (ステップ S8)。

(3) ユーザ B330 による署名検証

ユーザ B330 は、

$$s * R_1 = m * G + r_x * Y_A$$

が成立するかどうか判定することにより、送信者であるユーザ A310 の身元を確認する (ステップ S9)。これは、

$$\begin{aligned} s * R_1 &= [((m + r_x \times x_A) / k) \times k] * G \\ &= (m + r_x \times x_A) * G \\ &= m * G + (r_x \times x_A) * G \\ &= m * G + r_x * Y_A \end{aligned}$$

となることから明らかである。

【0009】

上記に示した楕円曲線上の離散対数問題を応用するエルガマル署名によるデジタル署名方式における公開鍵の生成、署名生成及び署名検証のそれぞれにおいて、楕円曲線上の点の冪倍の演算が行われる。

楕円曲線の演算公式については、

「Efficient elliptic curve exponentiation」 (Miyaji, Ono, and Cohen 著、Advances in cryptology-proceedings of ICICS'97, Lecture notes in computer science, 1997, Springer-verlag, 282-290.) に詳しく説明されている。

【0010】

楕円曲線の方程式を

$$y^2 = x^3 + a \times x + b$$

とする。楕円曲線上の任意の点 P の座標を (x_1, y_1) とする。この座標はアフィン座標と呼ばれている。

楕円曲線上における加算には、有限体 $GF(q)$ の逆元演算の処理を含むことが知られている。上記の論文では、射影座標と呼ばれる座標に触れているが、これは、

$$(x_1, y_1) \rightarrow (x_1, y_1, 1)$$

のように、2 項組座標を 3 項組座標に対応づけるものである。3 項組座標の場合、楕円曲線の加算には、有限体 $GF(q)$ の逆元演算の処理が含まれない。一般に有限体の逆元演算は、計算時間が長いため、3 項組座標がよく用いられる。

【0 0 1 1】

逆に、

$$(X, Y, Z) \rightarrow (X/Z, Y/Z)$$

のように、2 項組座標は 3 項組座標に対応づけられる。ここで、逆元演算が必要となる。

上記のエルガマル署名のステップ S 6 においては、2 項組座標を 3 項組座標に変換し、3 項組座標により楕円曲線上の加算を行い、加算結果の 3 項組座標をアフィン座標に変換する。したがって、3 項組座標からアフィン座標への変換において、逆元演算が必要になる。

(従来例 2 : 拡大体上の逆元演算)

以下において、従来の拡大体 $GF(q)$ ($q = p^n$ 、 p は素数、 n は正の整数) の逆元演算について説明する。

【0 0 1 2】

ここで、簡単のため、拡大体 $GF(q)$ の生成多項式を $f(g) = g^n - \beta$ とし、生成多項式の根を α とし、生成多項式の入力となる $GF(q)$ の元を

$$x = x_0 + x_1 \times \alpha + \cdots + x_{n-1} \times \alpha^{n-1} \text{ とする。}$$

(1) ステップ 1

$GF(q)$ の元 x を基にして、 y_i ($0 \leq i \leq n-1$) に関する以下の連立方

程式を生成する。

【0013】

$$\begin{aligned}
 x_0 y_0 + \beta x_{n-1} y_1 + \beta x_{n-2} y_2 + \cdots + \beta x_1 y_{n-1} &= 1 \\
 x_1 y_0 + x_0 y_1 + \beta x_{n-1} y_2 + \cdots + \beta x_2 y_{n-1} &= 0 \\
 x_2 y_0 + x_1 y_1 + x_0 y_2 + \cdots + \beta x_3 y_{n-1} &= 0 \\
 &\vdots \\
 x_{n-2} y_0 + x_{n-3} y_1 + x_{n-4} y_2 + \cdots + \beta x_{n-1} y_{n-1} &= 0 \\
 x_{n-1} y_0 + x_{n-2} y_1 + x_{n-3} y_2 + \cdots + x_0 y_{n-1} &= 0
 \end{aligned}$$

(2) ステップ2

生成された連立方程式の解 y_k ($k = 0, 1, \dots, n-1$) を求める。

(3) ステップ3

求めた解 y_k ($k = 0, 1, \dots, n-1$) を

逆元 $I = y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}$ に変換する。

【0014】

このようにして、拡大体 $GF(q)$ 上の元の逆元が求められる。

次に、上記のようにして逆元演算ができる根拠について説明する。

上記の逆元 I と元 x について、

$$x I = 1 \pmod{f(g)}$$

という関係を満たすとき、

$$\begin{aligned}
 x I = & x_0 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}) \\
 & + x_1 \alpha (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}) \\
 & + x_2 \alpha^2 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}) \\
 & \vdots \\
 & + x_{n-1} \alpha^{n-1} (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})
 \end{aligned}$$

であり、

$$\alpha^n = \beta \pmod{f(g)}$$

であるので、

$$\begin{aligned}
 x I = & x_0 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}) \\
 & + x_1 (y_0 \alpha + y_1 \alpha^2 + \cdots + y_{n-1} \beta)
 \end{aligned}$$

$$+x_2 (y_0 \alpha^2 + y_1 \alpha^3 + \dots + y_{n-1} \alpha \beta)$$

...

$$+x_{n-1} (y_0 \alpha^{n-1} + y_1 \beta + \dots + y_{n-1} \alpha^{n-2} \beta)$$

であり、 α の降冪の順に整理すると

$$xI = x_0 y_0 + \beta x_{n-1} x y_1 + \dots + \beta x_1 y_{n-1}$$

$$+ \alpha (x_1 y_0 + x_0 x y_1 + \dots + \beta x_2 y_{n-1})$$

$$+ \alpha^2 (x_2 y_0 + x_1 y_1 + \dots + \beta x_3 y_{n-1})$$

...

$$+ \alpha^{n-1} (x_{n-1} y_0 + x_{n-2} y_1 + \dots + x_0 y_{n-1})$$

である。

【0015】

ここで、 xI が1に等しいので、上記ステップ1において生成された連立方程式を導くことができる。

したがって、拡大体 $GF(q)$ の逆元を求めることは、基礎体 $GF(p)$ 上の連立方程式を解くことと等しい。

また、上記例では、 $g^n - \beta$ の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

(従来例3：基礎体 $GF(p)$ 上の連立方程式の解法)

以下において、基礎体 $GF(p)$ 上の連立方程式の従来解法について説明する。この解法は、ガウスの消去法と呼ばれる。ガウスの消去法については、「コンピュータによる数値計算」(水上孝一編著、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ)に詳しく述べられている。

【0016】

x_k ($k=0, 1, 2, \dots, n-1$) に対する連立方程式を、

$$a_{11}x_0 + a_{12}x_1 + \dots + a_{1n}x_{n-1} = b_1$$

$$a_{21}x_0 + a_{22}x_1 + \dots + a_{2n}x_{n-1} = b_2$$

...

$$a_{n1}x_0 + a_{n2}x_1 + \dots + a_{nn}x_{n-1} = b_n$$

とし、この解を求める。

(ステップ1)

行列M、ベクトルvを以下のようにおく。

【0017】

【数7】

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

$$v = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

【0018】

また、ベクトルXを次のようにおく。

【0019】

【数8】

$$X = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}$$

【0020】

上記の連立方程式は、次のように表現できる。

$$MX = v$$

行列Mを三角化するように、行列M、ベクトルvを変換し、それぞれ行列M'

、ベクトル v' を生成する。ここで、三角化とは、行列の対角成分より下の成分がすべて 0 となるような変換をいう。また、このような行列を上三角行列と呼ぶ。

【0021】

次に上記の従来の三角化の手順について、図 10 に示すフローチャートを用いて説明する。

カウンタ j に 1 を設定する (ステップ S21)。次に、 a_{jj} の逆元 I_j を算出し (ステップ S22)、 a_{jj} に 1 を設定し (ステップ S23)、 $j+1 \leq k \leq n$ に対して、 $a_{jk} = a_{jk} \times I_j$ 、 $b_j = b_j \times I_j$ とする (ステップ S24)。次にカウンタ $i = \text{カウンタ } j + 1$ とする (ステップ S25)。

【0022】

a_{ij} に 0 を設定し (ステップ S26)、 $j+1 \leq k \leq n$ に対して、 $a_{ik} = a_{ik} - a_{ij} \times a_{jk}$ とし (ステップ S27)、 $b_i = b_i - a_{ij} \times b_j$ とする (ステップ S28)。次に、 $i = n$ であるか否かを判断し、 $i = n$ でなければ (ステップ S29)、カウンタ i に 1 を加算して (ステップ S31)、制御をステップ S26 へ戻す。 $i = n$ であれば (ステップ S29)、 $j = n$ であるか否かを判断し、 $j = n$ でなければ (ステップ S30)、カウンタ j に 1 を加算して (ステップ S32)、制御をステップ S22 へ戻す。 $j = n$ であれば (ステップ S30)、処理を終了する。

【0023】

このようにして得られた行列を M' 、ベクトルを v' とする。ここで、行列 M' の対角成分は 1 であり、行列 M' の対角成分より下の成分がすべて 0 である。

連立方程式 $M' X = v'$ と、連立方程式 $M X = v$ とは、同値の関係を有する。ここで、

【0024】

【数 9】

$$M' = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}$$

$$v' = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix}$$

【0025】

とする。

(ステップ2)

生成された行列 M' 、ベクトル v' を用いて、次に示すようにして、連立方程式 $M' X = v'$ の解を求める。

カウンタ c に $n-1$ 、 \cdots 、 1 、 0 の値をこの順に設定し、カウンタ c の各値について、

$$c = n-1 \text{ のとき、} \quad y_c = d_{c+1}$$

$c \neq n-1$ のとき、

【0026】

【数 10】

$$y_c = d_{c+1} - \sum_{i=c+1}^{n-1} (C_{c+1 \ i+1} \times y_{i-1})$$

【0027】

を算出する。

(具体例)

従来例3を適用する具体例を以下に示す。

なお、この具体例は、三角化変換を分かりやすく説明するための例である。暗号通信システムやデジタル署名システムにおいて実際に使用される例ではないので注意を要する。

【0028】

素数 $p = 31$ 、生成多項式 $f(g) = g^5 - 2$ 、 $GF(q)$ の元 $x = 5\alpha^4 + 29\alpha^3 + 6\alpha^2 + 19\alpha + 17$ とする。

$$\begin{aligned} x \times \alpha &= 5\alpha^5 + 29\alpha^4 + 6\alpha^3 + 19\alpha^2 + 17\alpha \\ &= 29\alpha^4 + 6\alpha^3 + 19\alpha^2 + 17\alpha + 5 \times 2 \\ x \times \alpha^2 &= 29\alpha^5 + 6\alpha^4 + 19\alpha^3 + 17\alpha^2 + 10\alpha \\ &= 6\alpha^4 + 19\alpha^3 + 17\alpha^2 + 10\alpha + 29 \times 2 \\ x \times \alpha^3 &= 6\alpha^5 + 19\alpha^4 + 17\alpha^3 + 10\alpha^2 + 27\alpha \\ &= 19\alpha^4 + 17\alpha^3 + 10\alpha^2 + 27\alpha + 6 \times 2 \\ x \times \alpha^4 &= 19\alpha^5 + 17\alpha^4 + 10\alpha^3 + 27\alpha^2 + 12\alpha \\ &= 17\alpha^4 + 10\alpha^3 + 27\alpha^2 + 12\alpha + 19 \times 2 \end{aligned}$$

であるので、連立方程式は、図 11 (a) に示すようになる。係数行列 301 は、5 行 5 列の成分からなり、定数ベクトル 302 は、5 個の成分からなる。

【0029】

この連立方程式において、一次方程式

$$17x_0 + 10x_1 + 27x_2 + 12x_3 + 7x_4 = 1$$

を変換を行う際に軸となる軸方程式と呼び、この連立方程式の他の方程式を変換の対象となる対象方程式と呼ぶ。

次に、逆元演算を行う。

【0030】

$$1 / 17 \bmod 31 = 11$$

続けて、次の演算を行う。

$$10 \times 11 \bmod 31 = 17$$

$$27 \times 11 \bmod 31 = 18$$

$$12 \times 11 \bmod 31 = 8$$

$$7 \times 11 \bmod 31 = 15$$

$$1 \times 11 \bmod 31 = 11$$

従って、連立方程式は、図 11 (b) に示すようになる。ここで、係数行列 3 1 1 の 1 列 1 行の成分は、1 となる。この図の係数行列 3 1 1 及び定数ベクトル 3 1 2 において、枠で囲まれた数字は、図 11 (a) に示す係数行列 3 0 1 及び定数ベクトル 3 0 2 から変化した係数を示す。以下の図においても同様である。

【0031】

ここで、上記の逆元演算 $1/17 \bmod 31 = 11$ の詳細について以下に説明する。

この逆元演算においては、

$$a \times 17 + b \times 31 = 1$$

を満たす a を拡張 GCD 法によって求め、 a の値を前記逆元演算の演算値とする。

【0032】

拡張 GCD 法は、乗算や加算を繰り返し行うため、一般に計算量が多い。

拡張 GCD 法については、「A Course in Computational Algebraic Number Theory」(H. Cohen 著, Graduate texts in mathematics 138, 1996, Springer-Verlag, 16~19 ページ) に説明されている。

次に、係数行列 3 1 1 の 1 列 2 行の成分がそれぞれ 0 となるように、

$$17 - 17 \times 19 = 4 \quad \bmod 31$$

$$10 - 18 \times 19 = 9 \quad \bmod 31$$

$$27 - 8 \times 19 = 30 \quad \bmod 31$$

$$12 - 15 \times 19 = 6 \quad \bmod 31$$

$$0 - 11 \times 19 = 8 \quad \bmod 31$$

を演算する。同様にして、係数行列 3 1 1 の 1 列 3 行~5 行の成分がそれぞれ 0 となるように、係数行列 3 1 1 を係数行列 3 2 1 に変換し、ベクトル 3 1 2 をベクトル 3 2 2 に変換し、図 11 (c) に示す連立方程式が得られる。

【0033】

次に、行列 3 2 1 の 2 列 2 行の成分が 1 となるように、係数行列 3 2 1 を係数行列 3 3 1 に変換し、ベクトル 3 2 2 をベクトル 3 3 2 に変換し、図 11 (d)

に示す連立方程式が得られる。さらに、前記と同様にして、係数行列 3 3 1 の 2 列 3 行～5 行の成分が 0 となるように、係数行列 3 3 1 を係数行列 3 4 1 に変換し、ベクトル 3 3 2 をベクトル 3 4 2 に変換し、図 1 1 (e) に示す連立方程式が得られる。

【0 0 3 4】

以下同様にして、図 1 1 (f) に示す係数行列 3 5 1 のように 3 列 3 行の成分は 1 となり、図 1 1 (g) に示す係数行列 3 6 1 のように 3 列 4 行～5 行の成分は 0 となる。さらに、図 1 1 (h) に示す係数行列 3 7 1 のように 4 列 4 行の成分は 1 となり、図 1 1 (i) に示す係数行列 3 8 1 のように 4 列 5 行の成分は 0 となる。最後に、図 1 1 (j) に示す係数行列 3 9 1 のように 5 列 5 行の成分は 1 となる。

【0 0 3 5】

このようにして、係数行列が上三角行列に変換される。

次に、

$$y_4 = 29$$

$$\begin{aligned} y_3 &= 15 - 21 \times 29 \\ &= 26 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_2 &= 11 - 4 \times 26 - 28 \times 29 \\ &= 25 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_1 &= 2 - 10 \times 25 - 23 \times 26 - 17 \times 29 \\ &= 25 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_0 &= 11 - 17 \times 25 - 18 \times 25 - 8 \times 26 - 15 \times 29 \\ &= 12 \pmod{31} \end{aligned}$$

を算出する。

(計算量の評価)

従来例 3 の全計算量は、次に示すようになる。ここで、基礎体の乗算、逆元演算の計算量をそれぞれ、Mul、Inv とする。

【0 0 3 6】

上記のステップ 1 について、カウンタ j に対するループ内の計算量の内訳は次

のようになる。

(a) ステップ S 2 2 において、1 回の逆元演算が必要であるので、1 Inv

(b) ステップ S 2 4 において、 $(n - (j + 1) + 1) + 1 = n - j + 1$ 回の乗算が必要であるので、 $(n - j + 1) \times \text{Mul}$

(c) カウンタ i が変化する範囲 $j + 1 \sim n$ において、以下のとおり。

【0037】

(c-1) ステップ S 2 7 において、 $(n - (j + 1) + 1)$ 回の乗算が必要であるので、 $(n - j) \times \text{Mul}$

(c-2) ステップ S 2 8 において、1 回の乗算が必要であるので、1 Mul

(c-1) と (c-2) とを $(n - (j + 1) + 1) = (n - j)$ 回行うので、(c) 全体では、 $(n - j) (n - j + 1) \times \text{Mul}$ となる。

【0038】

次に、(a)、(b)、(c) の合計は、 $(n - j + 1) (n - j + 1) \times \text{Mul} + 1 + 1 \text{ Inv}$

カウンタ j は、1 ~ n の範囲で変化するので、ステップ 1 全体の計算量は、

【0039】

【数 1 1】

$$\begin{aligned}
 & \sum_{j=1}^n ((n - j + 1) (n - j + 1) \times \text{Mul} + \text{Inv}) \\
 &= \sum_{j=1}^n (n - j + 1) (n - j + 1) \times \text{Mul} \\
 &+ \sum_{j=1}^n 1 \text{ Inv} \\
 &= \sum_{j=1}^n j^2 \times \text{Mul} + n \times \text{Inv} \\
 &= 1/6 \times n (n + 1) (2n + 1) + n \times \text{Inv}
 \end{aligned}$$

【0040】

となる。

上記のステップ2について、計算量は次のようになる。

カウンタ c に対して、 $(n - (c + 1) + 1) = (n - c)$ 回の乗算が必要であるので、 $(n - c) \times \text{Mul}$

カウンタ c は、 $1 \sim n$ の範囲で変化するので、ステップ2全体の計算量は、

【0041】

【数12】

$$\begin{aligned}
 & \sum_{c=1}^n (n - c) \times \text{Mul} \\
 &= \sum_{c=1}^n (c - 1) \times \text{Mul} \\
 &= \left(\sum_{c=1}^n c - \sum_{c=1}^n 1 \right) \times \text{Mul} \\
 &= (1/2 \times n(n+1) - n) \times \text{Mul} \\
 &= 1/2 \times n(n-1) \times \text{Mul}
 \end{aligned}$$

【0042】

従って、従来例3の全体の計算量は、

$$\begin{aligned}
 & (1/6 \times n(n+1)(2n+1) + 1/2 \times n(n-1)) \times \text{Mul} + n \times \text{Inv} \\
 &= 1/3 \times n \times (n^2 + 3n - 1) \times \text{Mul} + n \times \text{Inv}
 \end{aligned}$$

となる。

ここで、 $n=5$ 、 $|q|=160$ ($|q|$ は q のビットサイズ) の場合、一般的な計算機では、 $\text{Inv} = 40 \text{ Mul}$ であることが知られているので、従来例3の全体の計算量は、 $265 \times \text{Mul}$ である。

【0043】

【発明が解決しようとする課題】

以上説明したように、有限体上の連立方程式を解くことにより、拡大体上の逆元演算ができるものの、拡大体上の逆元演算の計算量は一般に大きいので、有限体上の連立方程式の求解及び拡大体上の逆元演算における計算量をさらに少なくしたいという要望がある。

【0044】

本発明は、上記の要望に鑑み、有限体上の連立方程式の求解法において、計算量を削減することができる有限体上の連立方程式の求解装置、求解方法、求解プログラムを記録している記録媒体、拡大体上の逆元演算における計算量を削減することができる拡大体上の逆元演算装置、逆元演算方法、逆元演算プログラムを記録している記録媒体、これらの装置を応用する通信システム及び記録媒体再生装置を提供することを目的とする。

【0045】

【課題を解決するための手段】

上記の目的を達成するために、本発明は、有限体 $GF(p)$ (p は素数) 上の n 元連立一次方程式 $Ax = b$ (n は正の整数、 A は n 行 n 列の成分からなる係数行列、 x は n 個の成分からなる変数ベクトル、 b は n 個の成分からなる定数ベクトル) の解を求める連立方程式求解装置であって、係数行列 A と定数ベクトル b とを記憶しているパラメタ記憶手段と、前記パラメタ記憶手段から係数行列 A と定数ベクトル b とを読み出し、読み出した係数行列 A 及び定数ベクトル b を三角化変換して方程式 $Ax = b$ と同値の関係を有する n 元連立一次方程式 $Cx = d$ の係数行列 C (C は n 行 n 列の成分からなる係数行列) 及び定数ベクトル d (d は n 個の成分からなる定数ベクトル) を生成する三角化変換手段と、前記三角化変換は、係数行列 A の各対角成分を 1 に変換しない、係数行列 A の上三角行列への変換であり、生成された係数行列 C の各対角成分の有限体 $GF(p)$ 上の逆元である対角逆元を生成する対角逆元演算手段と、生成された係数行列 C と定数ベクトル d と生成された各対角逆元とを用いて、方程式 $Ax = b$ の解として、方程式 $Cx = d$ の解を求める方程式求解手段とを備えることを特徴とする。

【0046】

ここで、前記三角化変換手段は、連続する 1 個以上の変換過程を介して前記方

程式 $Cx = d$ の係数行列 C 及び定数ベクトル d を生成し、前記各変換過程において、前記三角化変換手段は、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Ax = b$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $Cx = d$ であり、前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象となる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方程式である軸方程式とを含み、前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第 1 係数群と第 2 係数群とを定め、ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られ、前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし、前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くように構成してもよい。

【0047】

ここで、前記三角化変換手段は、前記各変換過程において、1 個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記三角化変換手段は、各副変換過程において、軸方程式の 0 でない係数を有する最高次の変数の係数から構成される群を第 1 係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の 0 でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第 2 係数群と定め、前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし、前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くように構

成してもよい。

【0048】

ここで、前記三角化変換手段は、前記各変換過程において、1個の係数群算出過程と、前記係数群算出過程後に1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記係数群算出過程において、前記三角化変換手段は、軸方程式及び1個以上の対象方程式の0でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる2個以上の値から構成される群を第1係数群と定め、前記第1係数群に含まれる値であって、軸方程式の0でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた1個以上の値から構成される群を第2係数群と定め、前記副変換過程において、前記三角化変換手段は、前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし、前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引くように構成してもよい。

【0049】

【発明の実施の形態】

1 第1の実施の形態

本発明の1の実施の形態としての逆元演算装置100について説明する。

1. 1 逆元演算装置100の構成

逆元演算装置100は、予め与えられた有限体 $GF(p)$ (p は素数)の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数)上の元 x の逆元 I を算出する。以下において、拡大体 $GF(q)$ の生成多項式を $g^n - \beta$ とし、その根を α とし、元 x を $x = x_0 + x_1 \alpha + \dots + x_{n-1} \alpha^{n-1}$ とする。ここで、 α は、 $GF(q)$ 上の元であり、 β 、 x_0 、 x_1 、 \dots 、 x_{n-1} は、 $GF(p)$ 上の元である。

【0050】

逆元演算装置100は、図1に示すように、パラメタ記憶部200、方程式生成部201、方程式求解部202、逆元変換部203及び逆元記憶部204から

構成される。

逆元演算装置100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクなどから構成されるコンピュータシステムであり、前記ハードディスクには、コンピュータプログラムが記憶されており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作する。これにより、方程式生成部201、方程式求解部202及び逆元変換部203は、それぞれの機能を達成する。

(1) パラメタ記憶部200

パラメタ記憶部200は、具体的には、ハードディスクから構成され、生成多項式のパラメタ β 、根 α 、 x_0 、 x_1 、 \dots 、 x_{n-1} をあらかじめ記憶している。

(2) 方程式生成部201

方程式生成部201は、パラメタ記憶部200からパラメタ β 、根 α 、 x_0 、 x_1 、 \dots 、 x_{n-1} を読み出し、読み出したパラメタ β 、根 α 、 x_0 、 x_1 、 \dots 、 x_{n-1} を用いて、 y_i ($i=0, 1, 2, \dots, n-1$)に関する連立方程式

$$x_0 y_0 + \beta x_{n-1} y_1 + \beta x_{n-2} y_2 + \dots + \beta x_1 y_{n-1} = 1$$

$$x_1 y_0 + x_0 y_1 + \beta x_{n-1} y_2 + \dots + \beta x_2 y_{n-1} = 0$$

$$x_2 y_0 + x_1 y_1 + x_0 y_2 + \dots + \beta x_3 y_{n-1} = 0$$

\dots

$$x_{n-1} y_0 + x_{n-2} y_1 + x_{n-3} y_2 + \dots + x_0 y_{n-1} = 0$$

のパラメタを生成する。

【0051】

前記連立方程式は、次のように表現できる。

$$AY = B$$

ここで、

【0052】

【数 13】

$$\text{行列 } A = \begin{bmatrix} x_0 & \beta x_{n-1} & \beta x_{n-2} & \cdots & \beta x_1 \\ x_1 & x_0 & \beta x_{n-1} & \cdots & \beta x_2 \\ x_2 & x_1 & x_0 & \cdots & \beta x_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & x_{n-2} & x_{n-3} & \cdots & x_0 \end{bmatrix}$$

$$\text{ベクトル } Y = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ \vdots \\ y_{n-1} \end{bmatrix}$$

$$\text{ベクトル } B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

【0053】

方程式生成部 201 が生成する連立方程式のパラメタは、行列 A 及びベクトル B である。方程式生成部 201 は、生成した行列 A とベクトル B とを方程式求解部 202 へ出力する。

また、方程式生成部 201 は、パラメタ記憶部 200 から根 α を読み出し、読み出した根 α を逆元変換部 203 へ出力する。

(3) 方程式求解部 202

方程式求解部 202 は、予め与えられた有限体 $GF(p)$ (p は素数) において、以下に示す x_i ($i = 1, 2, \dots, n$) に関する n 元連立一次方程式のパラメータ a_{ij} ($i, j = 1, 2, \dots, n$)、 b_k ($k = 1, 2, \dots, n$) が与えられたとき、 n 元連立一次方程式の $GF(p)$ 上の解を算出する。

【0054】

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2$$

...

$$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n$$

方程式求解部 202 は、図 1 に示すように、定数記憶部 101、方程式変換部 102、逆元演算部 103 及び方程式演算部 104 から構成される。

(定数記憶部 101)

定数記憶部 101 は、具体的には、RAM から構成され、方程式生成部 201 から行列 M とベクトル v とを受け取り、記憶する。ここで、

【0055】

【数 14】

$$\text{行列 } M = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

$$\text{ベクトル } v = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

【0056】

ここで、行列 M は、一例として、行列 A であり、ベクトル v は、一例として、ベクトル B である。

(方程式変換部 102)

方程式変換部 102 は、定数記憶部 101 から行列 M とベクトル v とを読み出し、読み出した行列 M 及びベクトル v を三角化変換して、方程式 $Mx = v$ と同値の関係を有する n 元連立一次方程式 $M'x = v'$ の行列 M' (M' は n 行 n 列の成分からなる係数行列) 及びベクトル v' (v' は n 個の成分からなる定数ベク

トル) を生成する。

【0 0 5 7】

前記三角化変換において、方程式変換部 1 0 2 は、行列 M の各対角成分が 1 に変換されないように、行列 M を上三角行列に変換する。

ここで、

【0 0 5 8】

【数 1 5】

$$\text{行列 } M' = \begin{bmatrix} C_{11} & C_{12} & \cdot & \cdot & \cdot & C_{1n} \\ C_{21} & C_{22} & \cdot & \cdot & \cdot & C_{2n} \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ C_{n1} & C_{n2} & \cdot & \cdot & \cdot & C_{nn} \end{bmatrix}$$

$$\text{ベクトル } v' = \begin{bmatrix} d_1 \\ d_2 \\ \cdot \\ \cdot \\ d_n \end{bmatrix}$$

【0 0 5 9】

前記三角化変換について以下に説明する。

前記三角化変換では、方程式 $Mx = v$ から、連続する 1 個以上の変換過程を介して前記 n 元連立一次方程式 $M'x = v'$ の行列 M' 及びベクトル v' を生成する。

前記各変換過程において、前記三角化変換手段は、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成する。ここで、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Mx = v$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $M'x = v'$ である。

【0 0 6 0】

前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象と

なる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方程式である軸方程式とを含む。

前記三角化変換では、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第 1 係数群と第 2 係数群とを定める。

【0061】

ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群である。前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られる。

【0062】

前記三角化変換では、前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とする。次に、前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く。

また、前記三角化変換では、前記各変換過程において、1 個以上の対象方程式をそれぞれ変換する前記対象方程式と同数の副変換過程とを含む。

【0063】

前記三角化変換では、各副変換過程において、軸方程式の 0 でない係数を有する最高次の変数の係数から構成される群を第 1 係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の 0 でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第 2 係数群と定める。

次に、前記三角化変換では、前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とする。また、前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引く。

【0064】

三角化変換のさらなる詳細については、後述する。

方程式変換部 102 は、生成した行列 M' 及びベクトル v' を方程式演算部 104 へ出力し、生成した行列 M' の対角成分 c_{ii} ($i = 1, 2, \dots, n$) を逆元演算部 103 へ出力する。

上記に説明するように、方程式変換部 102 は、行列 M を上三角行列になるように変換する。このとき、方程式の解を変化させないようにするため、ベクトル v も変化させている。従来法と異なる点は、対角成分を 1 にしないことである。

(逆元演算部 103)

逆元演算部 103 は、方程式変換部 102 から行列 M' の対角成分 c_{ii} ($i = 1, 2, \dots, n$) を受け取る。

【0065】

ここで、記述を簡単にするために、行列 M' の対角成分 c_{ii} ($i = 1, 2, \dots, n$) を、 m_i ($i = 1, 2, \dots, n$) と表現する。

逆元演算部 103 は、

【0066】

【数 16】

$$t_i = \prod_{k=1}^n m_k \quad (m_i \text{ を除く}) \mod p$$

$$(i = 1, 2, \dots, n)$$

【0067】

を次に示すようにして算出する。

逆元演算部 103 は、以下に記載した順序に従って算出する。

$$s_1 = m_1 \times m_2 \mod p$$

$$s_2 = s_1 \times m_3 \mod p$$

...

$$s_{n-3} = s_{n-4} \times m_{n-2} \mod p$$

$$t_n = s_{n-3} \times m_{n-1} \mod p$$

$$t_{n-1} = s_{n-3} \times m_n \mod p$$

$$\begin{aligned}
 s_n &= m_{n-1} \times m_n \bmod p, \quad t_{n-2} = s_{n-4} \times s_n \bmod p \\
 s_{n-1} &= m_{n-2} \times s_n \bmod p, \quad t_{n-3} = s_{n-5} \times s_{n-1} \bmod p \\
 s_{n-2} &= m_{n-3} \times s_{n-1} \bmod p, \quad t_{n-4} = s_{n-6} \times s_{n-2} \bmod p \\
 &\dots
 \end{aligned}$$

$$\begin{aligned}
 s_5 &= m_4 \times s_6 \bmod p, \quad t_3 = s_1 \times s_5 \bmod p \\
 s_4 &= m_3 \times s_5 \bmod p, \quad t_2 = m_1 \times s_4 \bmod p \\
 t_1 &= m_2 \times s_4 \bmod p
 \end{aligned}$$

次に、逆元演算部 103 は、予め与えられた k (k は、1、2、...、 n のうちのいずれか 1 個) を用いて、

$$t = t_k \times m_k \bmod p$$

を算出することにより、

【0068】

【数 17】

$$t = \prod_{i=1}^n m_i \bmod p$$

【0069】

を算出する。

次に、逆元演算部 103 は、

$$u = 1/t \bmod p$$

を算出する。

次に、逆元演算部 103 は、

$$\text{逆元 } I_i = u \times t_i \bmod p \quad (i = 1, 2, \dots, n)$$

を算出する。

【0070】

逆元演算部 103 は、算出した逆元 I_i ($i = 1, 2, \dots, n$) を方程式演算部 104 へ出力する。

以上説明したように、逆元演算部 103 は、方程式変換部 102 から出力され

た行列 M' の対角成分 c_{ii} ($i = 1, 2, \dots, n$)の $GF(p)$ 上の逆元 I_i ($i = 1, 2, \dots, n$)を計算し、出力する。

(方程式演算部104)

方程式演算部104は、方程式変換部102から行列 M' 及びベクトル v' を受け取り、逆元演算部103から逆元 I_i ($i = 1, 2, \dots, n$)を受け取る。

【0071】

方程式演算部104は、カウンタ $j = n-1, n-2, \dots, 2, 1, 0$ のように設定し、カウンタ j の各値について、行列 M' 、ベクトル v' 、逆元 I_i ($i = 1, 2, \dots, n$)を用いて、

$$j = n-1 \text{ のとき、 } y_j = I_{j+1} \times d_{j+1} \mod p$$

$j \neq n-1$ のとき、

【0072】

【数18】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1 i+1} \times y_i \right) \mod p$$

【0073】

を算出する。

次に、方程式演算部104は、算出した解 y_j ($j = 0, 1, 2, \dots, n-1$)を逆元変換部203へ出力する。

以下に、方程式演算部104により n 元連立一次方程式の解が得られる根拠を示す。

【0074】

方程式演算部104が受け取った行列 M' は上三角化行列であるので、方程式 $M'x = v'$ は、

$$c_{11}x_0 + c_{12}x_1 + c_{13}x_2 + \dots + c_{1n}x_{n-1} = d_1$$

$$c_{22}x_1 + c_{23}x_2 + \dots + c_{2n}x_{n-1} = d_2$$

...

$$c_{nn}x_{n-1} = d_n$$

のように表現でき、行列 M' の対角成分 c_{ii} ($i=1, 2, \dots, n$)の逆元は、それぞれ I_i ($i=1, 2, \dots, n$)である。

【0075】

従って、 x_{n-1} の解 y_{n-1} は、

$$y_{n-1} = I_n d_{n-1} \bmod p$$

である。

次に、 x_{n-2} の解 y_{n-2} は、

$$y_{n-2} = I_{n-1} (d_{n-1} - c_{n-1, n} y_{n-1}) \bmod p$$

である。同様にして、 x_j の解 y_j ($j=n-3, n-4, \dots, 0$)は、

【0076】

【数19】

$$y_j = I_{j+1} \times (d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1, i+1} \times y_i) \bmod p$$

【0077】

である。

(4) 逆元変換部203

逆元変換部203は、方程式求解部202の方程式演算部104から解 y_j ($j=0, 1, 2, \dots, n-1$)を受け取り、方程式生成部201から根 α を受け取る。逆元変換部203は、受け取った解 y_k ($j=0, 1, 2, \dots, n-1$)と根 α とを用いて、逆元 I を次の式により演算する。

【0078】

$$I = y_0 + y_1 \alpha + \dots + y_{n-1} \alpha^{n-1}$$

次に、逆元変換部203は、算出した逆元 I を逆元記憶部204に書き込む。

このようにして、拡大体 $GF(q)$ 上の元 x の逆元 I が得られる。

(5) 逆元記憶部 204

逆元記憶部 204 は、具体的にはハードディスクからなり、拡大体 $GF(q)$ 上の元 x の逆元 I を記憶する。

1. 2 逆元演算装置 100 の動作

逆元演算装置 100 の動作について説明する。

(1) 逆元演算装置 100 の全体の概要動作

逆元演算装置 100 の全体の概要動作について、図 2 に示すフローチャートを用いて説明する。

【0079】

方程式生成部 201 は、パラメタ記憶部 200 からパラメタ β 、根 α 、 x_0 、 x_1 、 \dots 、 x_{n-1} を読み出し、読み出したパラメタ β 、根 α 、 x_0 、 x_1 、 \dots 、 x_{n-1} を用いて、 y_i ($i=0, 1, 2, \dots, n-1$) に関する連立方程式 $AY=B$ のパラメタとして、行列 A 及びベクトル B を生成し、生成した行列 A とベクトル B とを方程式求解部 202 の定数記憶部 101 へ出力する（ステップ S101）。

【0080】

方程式求解部 202 の方程式変換部 102 は、定数記憶部 101 から行列 M とベクトル v とを読み出し、読み出した行列 M 及びベクトル v を三角化変換して、方程式 $Mx=v$ と同値の関係を有する n 元連立一次方程式 $M'x=v'$ の行列 M' 及びベクトル v' を生成する（ステップ S102）。

逆元演算部 103 は、行列 M' の対角成分 c_{ii} ($i=1, 2, \dots, n$) の逆元 I_i ($i=1, 2, \dots, n$) を算出する（ステップ S103）。

【0081】

方程式演算部 104 は、行列 M' 、ベクトル v' 及び逆元 I_i ($i=1, 2, \dots, n$) を用いて、 n 元連立一次方程式 $M'x=v'$ の解 y_j ($j=0, 1, 2, \dots, n-1$) を算出し、算出した解を逆元変換部 203 へ出力する（ステップ S104）。

逆元変換部 203 は、方程式求解部 202 から解 y_j ($j=0, 1, 2, \dots$

・、 $n-1$)を受け取り、方程式生成部201から根 α を受け取り、受け取った解と根 α とを用いて、拡大体 $GF(q)$ 上の元 x の逆元 I を算出し、算出した逆元 I を逆元記憶部204に書き込む(ステップS105)。

(2) 方程式変換部102の三角化変換の詳細の動作

方程式変換部102の三角化変換の詳細の動作について、図3に示すフローチャートを用いて説明する。

【0082】

方程式変換部102は、定数記憶部101から行列 M とベクトル v とを読み出し(ステップS111)、カウンタ j を1に設定する(ステップS112)。

次に、方程式変換部102は、行列 M の第 j 列の成分の中で $GF(p)$ 上で0でない成分を第 j 行から第 n 行まで探索し、はじめに発見した成分の行数を k とする(ステップS113)。さらに、 $k \neq j$ の場合に(ステップS114)、行列 M の第 k 行と第 j 行とを入れ換え(ステップS115)、ベクトル v の第 k 行と第 j 行とを入れ換える(ステップS116)。

【0083】

次に、方程式変換部102は、カウンタ i を $j+1$ に設定し(ステップS117)、方程式変換部102は、 a_{jj} (a_{jj} は、行列 M の j 行 j 列成分)と a_{ij} とを用いて、

$$a_{ij} = 0$$

$j+1 \leq k \leq n$ ($k = j+1, j+2, \dots, n$) に対して、

$$a_{ik} = a_{jj} a_{ik} - a_{ij} a_{jk}$$

$$b_i = a_{jj} b_i - a_{ij} b_j$$

のように設定する(ステップS118)。

【0084】

方程式変換部102は、 $i = n$ であるかを判定し、 $i \neq n$ であるなら(ステップS119)、カウンタ i に1を加算して(ステップS122)、ステップS118へ制御を戻す。 $i = n$ であるなら(ステップS119)、 $j = n-1$ であるかを判定し、 $j \neq n-1$ であるなら(ステップS120)、カウンタ j に1を加算して(ステップS123)、ステップS113へ制御を戻す。 $j = n-1$ である

なら（ステップ S120）、行列 M を行列 M' とし、ベクトル v をベクトル v' とする。

【0085】

以上説明したように、方程式変換部 102 には、カウンタ j を変化させることによる変換過程が含まれる。また、前記変換過程内には、カウンタ i を変化させることによる副変換過程が含まれる。

（方程式変換部 102 の検証）

方程式変換部 102 による三角化変換により生成される n 元連立一次方程式 $M'x = v'$ が、 n 元連立一次方程式 $Mx = v$ と同値の関係を有する根拠をについて以下に説明する。

【0086】

三角化変換において、 n 元連立一次方程式中の変換中の 1 個の n 元一次方程式について、変換前の行列を行列 M_{in} 、ベクトル v_{in} とし、変換後の行列を行列 M_{out} 、ベクトル v_{out} とし、行列 M_{in} の第 i 、 j 行の行ベクトルをそれぞれ、 L_i 、 L_j とする。

方程式変換部 102 において、

$$a_{jj} \times L_i - a_{ij} \times L_j$$

の計算を行い、この結果の行ベクトルを M_{out} の第 i 行とし、

$$a_{jj} \times b_i - a_{ij} \times b_j$$

の計算を行い、 v_{out} の第 i 行としている。 M_{out} の他の成分及び v_{out} の他の成分は、それぞれ M_{in} の他の成分及び v_{in} の他の成分と同じである。このとき、方程式

$$M_{in} \cdot x = v_{in}$$

と方程式

$$M_{out} \cdot x = v_{out}$$

が同じ解をもつことは、「コンピュータによる数値計算」（水上孝一編著、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ）から明らかである。

【0087】

また、カウンタ j に対して、 $j+1 \leq i \leq n$ を満たす i について、 a_{ij} を 0 と

している。この操作を j が 1 から n まで繰り返すので、行列の下三角部分が 0 になる。したがって、第 2 方程式変換部 102 は方程式の解を変化させずに、行列の三角化変換が行える。

(3) 逆元演算部 103 の動作

逆元演算部 103 の動作について、図 4 に示すフローチャートを用いて説明する。

【0088】

逆元演算部 103 は、方程式変換部 102 から行列 M' の対角成分 m_i ($i = 1, 2, \dots, n$) を受け取り (ステップ S140)、

【0089】

【数 20】

$$t_i = \prod_{k=1}^n m_k \quad (m_i \text{ を除く}) \bmod p$$

$$(i = 1, 2, \dots, n)$$

【0090】

を算出し (ステップ S142)、

予め与えられた k を用いて、

$$t = t_k \times m_k \bmod p$$

を算出し (ステップ S143)、

$$u = 1/t \bmod p$$

を算出し (ステップ S144)、

$$\text{逆元 } I_i = u \times t_i \bmod p \quad (i = 1, 2, \dots, n)$$

を算出し (ステップ S145)、算出した逆元 I_i ($i = 1, 2, \dots, n$)

を方程式演算部 104 へ出力する (ステップ S146)。

(4) 方程式演算部 104 の動作

方程式演算部 104 の動作について、図 5 に示すフローチャートを用いて説明する。

【0091】

方程式演算部104は、方程式変換部102から行列 M' 及びベクトル v' を受け取り、逆元演算部103から逆元 I_i ($i=1, 2, \dots, n$)を受け取る(ステップS161)。次に、方程式演算部104は、カウンタ j を $n-1$ に設定し(ステップS162)、

$$j = n-1 \text{ のとき、 } y_j = I_{j+1} \times d_{j+1} \mod p$$

$j \neq n-1$ のとき、

【0092】

【数21】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1 i+1} \times y_i \right) \mod p$$

【0093】

を算出する(ステップS163)。

方程式演算部104は、 $j=0$ であるか否かを判定し、 $j=0$ であるとき(ステップS164)、算出した解 y_j ($j=0, 1, 2, \dots, n-1$)を逆元変換部203へ出力する(ステップS166)。それ以外の場合は(ステップS164)、カウンタ j から1を減じ(ステップS165)、ステップS163へ制御を戻す。

1. 3 計算量の評価

方程式求解部202における計算量について説明する。

(1) 方程式変換部102における計算量

カウンタ j の値に対して、ループ(図3に示すフローチャートのステップS113～S119)内の処理の計算量は、次のようになる。

【0094】

カウンタ i の1個の値に対して

(a) ステップS118において、 $j+1 \leq k \leq n$ ($k=j+1, j+2, \dots$)

・ ・ ・、 n) に対して、 $a_{ik} = a_{jj} \times a_{ik} - a_{ij} \times a_{jk}$ の計算をする。従って、2 回の乗算を $(n - (j + 1) + 1) = (n - j)$ 回行うので、計算量は、 $2 \times (n - j) \times \text{Mul}$ 。

【0095】

(b) ステップ S118 において、 $b_i = a_{jj} \times b_i - a_{ij} \times b_j$ の計算をする。従って、2 回の乗算を行うので、計算量は、 2 Mul 。

カウンタ i は、 $j + 1 \sim n$ の範囲で変化するので、ループ (ステップ S113 \sim S119) 内の計算量は、

$$(2 \times (n - j + 1) \times \text{Mul}) \times (n - (j + 1) + 1) \\ = 2 \times (n - j) \times (n - j + 1) \times \text{Mul}$$

ステップ S112 \sim S120 において、カウンタ j は、 $1 \sim n - 1$ の範囲で変化するので、方程式変換部 102 全体の計算量は、

【0096】

【数 22】

$$\begin{aligned} & \sum_{j=1}^{n-1} (2 \times (n - j) \times (n - j + 1)) \text{ Mul} \\ &= 2 \text{ Mul} \times \sum_{j=1}^{n-1} j (j + 1) \\ &= 2 \text{ Mul} \times \left(\sum_{j=1}^{n-1} j^2 + \sum_{j=1}^{n-1} j \right) \\ &= 2 \text{ Mul} \times \left(1/6 \times n (n - 1) (2n - 1) \right. \\ & \quad \left. + 1/2 \times n (n - 1) \right) \\ &= 2 \text{ Mul} \times 1/6 \times n (n - 1) (2n - 1 + 3) \\ &= 1/3 \text{ Mul} \times n (n - 1) (2n + 2) \\ &= 2/3 \times n (n - 1) (n + 1) \text{ Mul} \end{aligned}$$

【0097】

(2) 逆元演算部 103 における計算量

(a) $s_1 \sim s_{n-3}$ 及び t_n を求めるために乗算が、 $n-2$ 回必要であるので、 $(n-2) \times \text{Mul}$

(b) t_{n-1} を求めるために 1 回の乗算が必要であるので、 Mul

(c) s_n と t_{n-2} 、 s_{n-1} と t_{n-3} 、 \dots 、 s_4 と t_2 を求めるために乗算が、 $2 \times (n-3)$ 回必要であるので、 $2 \times (n-3) \times \text{Mul}$

(d) t_1 を求めるために 1 回の乗算が必要であるので、 Mul

(e) t を求めるために 1 回の乗算が必要であるので、 Mul

(f) $u = 1/t \pmod{p}$ を求めるために、1 回の逆元演算が必要であるので、 Inv

(g) $I_i = u \times t_i \pmod{p}$ ($i = 1, 2, \dots, n$) を求めるために、 n 回の乗算が必要であるので、 $n \times \text{Mul}$

これらを合計すると、

$$\begin{aligned} & ((n-2) + 1 + 2(n-3) + 1 + 1 + n) \times \text{Mul} + \text{Inv} \\ &= (4n-5) \times \text{Mul} + \text{Inv} \end{aligned}$$

(3) 方程式演算部 104 における計算量

カウンタ j に対して、ループ内 (図 5 に示すフローチャートのステップ S163 ~ S165) の処理の計算量を見積もる。

【0098】

$j = n-1$ のとき、 $y_j = I_{j+1} \times d_{j+1} \pmod{p}$

$j \neq n-1$ のとき、

【0099】

【数 23】

$$y_j = I_{j+1} \times (d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1+i+1} \times y_i) \pmod{p}$$

【0100】

の計算を行うために、1 回の乗算 (右辺第 1 項) と $(n - (j+1) + 1)$ 回の

乗算が必要であるので、計算量は $(n-j+1) \times \text{Mul}$

カウンタ j は、 $1 \sim n$ の範囲で変化するので、方程式演算部 104 全体の計算量は、

【0101】

【数24】

$$\begin{aligned} & \sum_{j=1}^n (n-j+1) \times \text{Mul} \\ &= \sum_{j=1}^n j \times \text{Mul} \\ &= 1/2 \times n(n+1) \times \text{Mul} \end{aligned}$$

【0102】

(4) 具体例

具体例を以下に示す。

従来例3と同様に、素数 $p=31$ 、生成多項式 $f(g) = g^5 - 2$ 、 $GF(q)$ の元 $x = 5\alpha^4 + 29\alpha^3 + 6\alpha^2 + 19\alpha + 17$ とする。連立方程式は、従来例3と同様、図6(a)に示すようになる。

【0103】

次の演算をする。

$$\begin{aligned} a_{21} &= 0 \\ a_{22} &= 17 \times 17 - 19 \times 10 = 6 \quad \text{mod } 31 \\ a_{23} &= 17 \times 10 - 19 \times 27 = 29 \quad \text{mod } 31 \\ a_{24} &= 17 \times 27 - 19 \times 12 = 14 \quad \text{mod } 31 \\ a_{25} &= 17 \times 12 - 19 \times 7 = 9 \quad \text{mod } 31 \\ b_2 &= 17 \times 0 - 19 \times 1 = 12 \quad \text{mod } 31 \end{aligned}$$

$j=1$ ($i=2$) のとき

連立方程式は、図6(b)に示すようになる。ここで、係数行列 411 の1列2行の成分が0となっている。

【0104】

次に、 $j = 1$ の処理終了後、連立方程式は、図 6 (c) に示すようになる。ここで、係数行列 4 2 1 の 1 列 3 行～5 行の成分が 0 となっている。

次に、 $j = 2$ の処理終了後、連立方程式は、図 6 (d) に示すようになる。ここで、係数行列 4 3 1 の 2 列 3 行～5 行の成分が 0 となっている。

次に、 $j = 3$ の処理終了後、連立方程式は、図 6 (e) に示すようになる。ここで、係数行列 4 4 1 の 3 列 4 行～5 行の成分が 0 となっている。

【0105】

次に、 $j = 4$ の処理終了後、連立方程式は、図 6 (f) に示すようになる。ここで、係数行列 4 5 1 の 4 列 5 行の成分が 0 となっている。

次に、対角成分の逆元演算を行う。

$$s_1 = m_1 \times m_2 = 17 \times 6 = 9 \pmod{31}$$

$$s_2 = s_1 \times m_3 = 9 \times 17 = 29 \pmod{31}$$

$$t_5 = s_2 \times m_4 = 29 \times 6 = 19 \pmod{31}$$

$$t_4 = s_2 \times m_5 = 29 \times 30 = 2 \pmod{31}$$

$$s_5 = m_4 \times m_5 = 6 \times 30 = 25 \pmod{31}$$

$$t_3 = s_1 \times s_5 = 9 \times 25 = 8 \pmod{31}$$

$$s_4 = m_3 \times s_5 = 17 \times 25 = 22 \pmod{31}$$

$$t_2 = m_1 \times s_4 = 17 \times 22 = 2 \pmod{31}$$

$$t_1 = m_2 \times s_4 = 6 \times 22 = 8 \pmod{31}$$

$$t = m_1 \times t_1 = 17 \times 8 = 12 \pmod{31}$$

$$u = 1/t = 1/12 = 13 \pmod{31} \quad (\text{逆元演算はこの1回のみである。})$$

$$I_1 = u \times t_1 = 13 \times 8 = 11 \pmod{31}$$

$$I_2 = u \times t_2 = 13 \times 2 = 26 \pmod{31}$$

$$I_3 = u \times t_3 = 13 \times 8 = 11 \pmod{31}$$

$$I_4 = u \times t_4 = 13 \times 2 = 26 \pmod{31}$$

$$I_5 = u \times t_5 = 13 \times 19 = 30 \pmod{31}$$

次に、方程式を解く。

$$y_4 = I_5 \times d_5 = 30 \times 2 = 29 \pmod{31}$$

$$\begin{aligned} y_3 &= I_4 \times (d_4 - c_{45} \times y_4) \\ &= 26 \times (28 - 2 \times 29) = 26 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_2 &= I_3 \times (d_3 - c_{34} \times y_3 - c_{35} \times y_4) \\ &= 11 \times (1 - 6 \times 26 - 11 \times 29) = 25 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_1 &= I_2 \times (d_2 - c_{23} \times y_2 - c_{24} \times y_3 - c_{25} \times y_4) \\ &= 26 \times (12 - 29 \times 25 - 14 \times 26 - 9 \times 29) \\ &= 25 \pmod{31} \end{aligned}$$

$$\begin{aligned} y_0 &= I_1 \times (d_1 - c_{12} \times y_1 - c_{13} \times y_2 - c_{14} \times y_3 - c_{15} \times y_4) \\ &= 11 \times (1 - 10 \times 25 - 27 \times 25 - 12 \times 26 - 7 \times 29) \\ &= 12 \pmod{31} \end{aligned}$$

(5) 方程式求解部 202 全体における計算量

従って、方程式求解部 202 全体における計算量は、

$$\begin{aligned} & 2/3 \times n(n-1)(n+1) \text{ Mul} \\ & + (4n-5) \times \text{Mul} + \text{Inv} \\ & + 1/2 \times n(n+1) \times \text{Mul} \\ & = 1/6 (4n^3 + 3n^2 + 23n - 30) \text{ Mul} + \text{Inv} \end{aligned}$$

ここで、 $n=5$ 、 $|q|=160$ ($|q|$ は q のビットサイズ) の場合、一般的な計算機では、 $\text{Inv} = 40 \text{ Mul}$ であるとする、方程式求解部 202 における計算量は、 $150 \times \text{Mul}$ である。

【0106】

このように、本発明の方程式求解部 202 による計算量は、従来の方程式求解装置と比較すると、明らかに少なくなる。したがって、連立方程式の求解を少ない計算量で行える有限体上の連立方程式求解装置を提供することができ、この実用的価値は非常に大きい。

また、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ 上の元 x の逆元 I を算出する逆元演算装置において、少ない計算量で逆元演算を行うことができる。

(6) 適用例

実際に暗号通信システム、デジタル署名通信システム及び誤り訂正通信システムなどの通信システムにおいて、適用される一例としてのパラメタを示す。

【0107】

素数 $p = 2^{31} - 1$ 、 $q = p^n$ 、 $n = 5$ 、生成多項式 $f(g) = g^5 - g - 8$

$F(q)$ の元 $x = x_0 + x_1 \times \alpha + x_2 \times \alpha^2 + x_3 \times \alpha^3 + x_4 \times \alpha^4$

に対して、連立方程式は以下のように設定される。

【0108】

【数25】

$$\begin{pmatrix} x_0 & 8x_4 & 8x_3 & 8x_2 & 8x_1 \\ x_1 & x_0+x_4 & x_3+8x_4 & x_2+8x_3 & x_1+8x_2 \\ x_2 & x_1 & x_0+x_4 & x_3+8x_4 & x_2+8x_3 \\ x_3 & x_2 & x_1 & x_0+x_4 & x_3+8x_4 \\ x_4 & x_3 & x_2 & x_1 & x_0+x_4 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

【0109】

ここで、 p 、 x_0 、 \dots 、 x_4 、 y_0 、 \dots 、 y_4 は、それぞれ31ビットであり、 q 、 x は、155ビットである。

2 その他の実施の形態

本発明に係るその他の実施の形態について説明する。

2. 1 変形例

方程式求解部202の方程式変換部102の変形例としての方程式変換部102aについて説明する。

【0110】

方程式変換部102aは、方程式変換部102で説明した前記各変換過程において、1個の係数群算出過程と、前記係数群算出過程後に1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含む。

前記係数群算出過程において、方程式変換部102aは、軸方程式及び1個以上の対象方程式の0でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる2個以上の値から構成される群を第1係数群と定め、前記第1係数群に含まれる値であって、軸方程式の0でない

い係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた1個以上の値から構成される群を第2係数群と定める。

【0111】

前記副変換過程において、方程式変換部102aは、前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし、前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引く。

【0112】

方程式変換部102aの動作について、図7に示すフローチャートを用いて説明する。図7に示すフローチャートは、図3のフローチャートのステップS118に代えて、ステップS118a～S118cを含む。

以下に、ステップS118a～S118cについて説明する。他のステップは、図3のフローチャートのステップと同じであるので、説明を省略する。

【0113】

方程式変換部102aは、ステップ118aにおいて、 $j \leq k \leq n$ なる k ($k = j, j+1, \dots, n$) に対して、

【0114】

【数26】

$$h_k = \prod_{m=j}^n a_{mk} \quad (a_{kj} \text{ 除く})$$

【0115】

を算出する。

また、方程式変換部102aは、ステップ118bにおいて、 $j+1 \leq k \leq n$ なる k ($k = j+1, j+2, \dots, n$) に対して、

$$\begin{aligned} w_k &= h_j \times a_{jk} \\ e &= h_j \times b_j \end{aligned}$$

を算出する。

【0116】

また、方程式変換部102aは、ステップ118cにおいて、

$a_{ij}=0$ とし、

$j+1 \leq k \leq n$ なる k ($k=j+1, j+2, \dots, n$) に対して、

$a_{ik}=h_i \times a_{ik}-w_k$ を算出し、

$b_i=h_i \times b_i-e$ を算出する。

(具体例)

具体例を以下に示す。

【0117】

従来例3と同様に、素数 $p=31$ 、生成多項式 $f(g)=g^5-2$ 、 $GF(q)$ の元 $x=5\alpha^4+29\alpha^3+6\alpha^2+19\alpha+17$ とする。連立方程式は、従来例3と同様、図8(a)に示すようになる。

$j=1$ のとき、

$$s_1 = a_{11} \times a_{21} = 17 \times 19 = 13 \pmod{31}$$

$$s_2 = s_1 \times a_{31} = 13 \times 6 = 16 \pmod{31}$$

$$h_5 = s_2 \times a_{41} = 16 \times 29 = 30 \pmod{31}$$

$$h_4 = s_2 \times a_{51} = 16 \times 5 = 18 \pmod{31}$$

$$s_5 = a_{41} \times a_{51} = 29 \times 5 = 21 \pmod{31}$$

$$h_3 = s_1 \times s_5 = 13 \times 21 = 25 \pmod{31}$$

$$s_4 = a_{31} \times s_5 = 6 \times 21 = 2 \pmod{31}$$

$$h_2 = a_{11} \times s_4 = 17 \times 2 = 3 \pmod{31}$$

$$h_1 = a_{21} \times s_4 = 19 \times 2 = 7 \pmod{31}$$

を算出し、

$$w_2 = h_1 \times a_{12} = 7 \times 10 = 8 \pmod{31}$$

$$w_3 = h_1 \times a_{13} = 7 \times 27 = 3 \pmod{31}$$

$$w_4 = h_1 \times a_{14} = 7 \times 12 = 22 \pmod{31}$$

$$w_5 = h_1 \times a_{15} = 7 \times 7 = 18 \pmod{31}$$

$$e = h_1 \times b_1 = 7 \times 1 = 7 \pmod{31}$$

を算出する。

【0118】

次に、 $i = 2$ ($j = 1$) のとき

$$a_{21} = 0$$

$$a_{22} = h_2 \times a_{22} - w_2 = 3 \times 17 - 8 = 12 \pmod{31}$$

$$a_{23} = h_2 \times a_{23} - w_3 = 3 \times 10 - 3 = 27 \pmod{31}$$

$$a_{24} = h_2 \times a_{24} - w_4 = 3 \times 27 - 22 = 28 \pmod{31}$$

$$a_{25} = h_2 \times a_{25} - w_5 = 3 \times 12 - 18 = 18 \pmod{31}$$

$$b_2 = h_2 \times b_2 - e = 3 \times 0 - 7 = 24 \pmod{31}$$

このように、上記の第1の実施形態と異なり、 a_{ik} を求めるために、乗算を1回のみ行うので、計算量が少なくなる。(第1の実施形態では、乗算を2回行う。)

こうして、図8(b)に示す連立方程式が得られる。ここで、1列2行の成分が0である。

【0119】

次に、 $j = 1$ の処理終了後、図8(c)に示す連立方程式が得られる。ここで、1列3行～5行の成分が0である。

次に、 $j = 2$ のとき

$$s_1 = a_{22} \times a_{32} = 12 \times 2 = 24 \pmod{31}$$

$$h_5 = s_1 \times a_{42} = 24 \times 7 = 13 \pmod{31}$$

$$h_4 = s_1 \times a_{52} = 24 \times 25 = 11 \pmod{31}$$

$$s_4 = a_{42} \times a_{52} = 7 \times 25 = 20 \pmod{31}$$

$$h_3 = a_{22} \times s_4 = 12 \times 20 = 23 \pmod{31}$$

$$h_2 = a_{32} \times s_4 = 2 \times 20 = 9 \pmod{31}$$

を演算し、

$$w_3 = h_2 \times a_{23} = 9 \times 27 = 26 \pmod{31}$$

$$w_4 = h_2 \times a_{24} = 9 \times 28 = 4 \pmod{31}$$

$$w_5 = h_2 \times a_{25} = 9 \times 18 = 7 \pmod{31}$$

$$e = h_2 \times b_2 = 9 \times 24 = 30 \pmod{31}$$

を演算する。

【0120】

次に、 $j = 2$ の処理終了後、図 8 (d) に示す連立方程式が得られる。ここで、2 列 3 行～5 行の成分が 0 である。

次に、 $j = 3$ のとき、

$$h_5 = a_{33} \times a_{43} = 8 \times 14 = 19 \pmod{31}$$

$$h_4 = a_{33} \times a_{53} = 8 \times 12 = 3 \pmod{31}$$

$$h_3 = a_{43} \times a_{53} = 14 \times 12 = 13 \pmod{31}$$

を演算し、

$$w_4 = h_3 \times a_{34} = 13 \times 1 = 13 \pmod{31}$$

$$w_5 = h_3 \times a_{35} = 13 \times 7 = 29 \pmod{31}$$

$$e = h_3 \times b_3 = 13 \times 26 = 28 \pmod{31}$$

を演算する。

【0121】

次に、 $j = 3$ の処理終了後、図 8 (e) に示す連立方程式が得られる。ここで、3 列 4 行～5 行の成分が 0 である。

次に、 $j = 4$ のとき

$$h_5 = a_{44} = 16 \pmod{31}$$

$$h_4 = a_{54} = 14 \pmod{31}$$

を算出し、

$$w_5 = h_4 \times a_{45} = 14 \times 26 = 23 \pmod{31}$$

$$e = h_4 \times b_4 = 14 \times 23 = 12 \pmod{31}$$

を算出する。

【0122】

次に、 $j = 4$ の処理終了後、図 8 (f) に示す連立方程式が得られる。ここで、4 列 5 行の成分が 0 である。

ここで、行列 $C = A$ 、ベクトル $D = B$ とする。

次に、対角成分の逆元演算を行う。

$$s_1 = m_1 \times m_2 = 17 \times 12 = 18 \pmod{31}$$

$$\begin{aligned}
s_2 &= s_1 \times m_3 = 18 \times 8 = 20 \pmod{31} \\
t_5 &= s_2 \times m_4 = 20 \times 16 = 10 \pmod{31} \\
t_4 &= s_2 \times m_5 = 20 \times 22 = 6 \pmod{31} \\
s_5 &= m_4 \times m_5 = 16 \times 22 = 11 \pmod{31} \\
t_3 &= s_1 \times s_5 = 18 \times 11 = 12 \pmod{31} \\
s_4 &= m_3 \times s_5 = 8 \times 11 = 26 \pmod{31} \\
t_2 &= m_1 \times s_4 = 17 \times 26 = 8 \pmod{31} \\
t_1 &= m_2 \times s_4 = 12 \times 26 = 2 \pmod{31} \\
t &= m_1 \times t_1 = 17 \times 2 = 3 \pmod{31} \\
u &= 1/t = 1/3 = 21 \pmod{31}
\end{aligned}$$

を演算する。逆元演算はこの1回のみである。

【0123】

$$\begin{aligned}
I_1 &= u \times t_1 = 21 \times 2 = 11 \pmod{31} \\
I_2 &= u \times t_2 = 21 \times 8 = 13 \pmod{31} \\
I_3 &= u \times t_3 = 21 \times 12 = 4 \pmod{31} \\
I_4 &= u \times t_4 = 21 \times 6 = 2 \pmod{31} \\
I_5 &= u \times t_5 = 21 \times 10 = 24 \pmod{31}
\end{aligned}$$

を演算する。

【0124】

次に方程式を解く。

$$\begin{aligned}
y_4 &= I_5 \times d_5 = 24 \times 18 = 29 \pmod{31} \\
y_3 &= I_4 \times (d_4 - c_{42} \times y_4) \\
&= 2 \times (23 - 26 \times 29) = 26 \pmod{31} \\
y_2 &= I_3 \times (d_3 - c_{34} \times y_3 - c_{35} \times y_4) \\
&= 4 \times (26 - 1 \times 26 - 7 \times 29) = 25 \pmod{31} \\
y_1 &= I_2 \times (d_2 - c_{23} \times y_2 - c_{24} \times y_3 - c_{25} \times y_4) \\
&= 13 \times (24 - 27 \times 25 - 28 \times 26 - 18 \times 29) \\
&= 25 \pmod{31} \\
y_0 &= I_1 \times (d_1 - c_{12} \times y_1 - c_{13} \times y_2 - c_{14} \times y_3 - c_{15} \times y_4)
\end{aligned}$$

$$\begin{aligned}
 &= 11 \times (1 - 10 \times 25 - 27 \times 25 - 12 \times 26 - 7 \times 29) \\
 &= 12 \pmod{31}
 \end{aligned}$$

(方程式変換部 102a の計算量の評価)

図*に示すフローチャートにおけるカウンタ j に対するループ内 (ステップ S113～ステップ S119) の計算量を見積もる。

【0125】

ステップ S118a において、 h_k ($k = j, j+1, \dots, n$) を求めるために、 $(3 \times (n - j + 1) - 6)$ 回の乗算が必要であるので、計算量は、 $(3 \times (n - j + 1) - 6) \times \text{Mul}$ である。

ステップ S118b において、 w_k ($k = j+1, j+2, \dots, n$) と e とを求めるために、 $(n - (j + 1) + 1 + 1)$ 回の乗算が必要であるので、計算量は、 $(n - j + 1) \times \text{Mul}$ である。

【0126】

ステップ S118c において、カウンタ i の 1 個の値に対して、

(a) $j+1 \leq k \leq n$ ($k = j+1, j+2, \dots, n$) について、 $a_{ik} = h_i \times a_{ik} - w_k$ の計算をする。1 回の乗算を $(n - (j + 1) + 1) = (n - j)$ 回行うので、計算量は $(n - j) \times \text{Mul}$ である。

(b) $b_i = h_i \times b_i - e$ の計算をする。1 回の乗算を行うので、計算量は 1 Mul である。

【0127】

カウンタ i は、 $j+1 \sim n$ の範囲で変化するので、ループ内の計算量は、

$$\begin{aligned}
 &((n - j + 1) \times \text{Mul}) \times (n - (j + 1) + 1) \\
 &= (n - j) \times (n - j + 1) \times \text{Mul}
 \end{aligned}$$

ステップ S118a～S118c の計算量の合計は、

$$((3 \times (n - j + 1) - 6) + (n - j + 1) + (n - j) (n - j + 1)) \times \text{Mul}$$

$$= (4 \times (n - j + 1) - 6 + (n - j) (n - j + 1)) \times \text{Mul}$$

$$= ((n - j + 4) (n - j + 1) - 6) \times \text{Mul}$$

カウンタ j は、 $1 \sim n-1$ の範囲で変化するので、方程式変換部 102a 全体

の計算量は、

【0128】

【数27】

$$\begin{aligned}
 & \sum_{j=1}^{n-1} ((n-j+4)(n-j+1)-6) \text{Mul} \\
 = & \text{Mul} \times \sum_{j=1}^{n-1} ((j+4)(j+1)-6) \\
 = & \text{Mul} \times \left(\sum_{j=1}^{n-1} j^2 + 5 \times \sum_{j=1}^{n-1} j - 2 \times \sum_{j=1}^{n-1} 1 \right) \\
 = & \text{Mul} \times (1/6 \times n(n-1)(2n-1) \\
 & + 5/2 \times n(n-1) - 2(n-1)) \\
 = & \text{Mul} \times (1/6 \times n(n-1)(2n-1+15) \\
 & - 2(n-1)) \\
 = & \text{Mul} \times (1/6 \times n(n-1)(2n+14) \\
 & - 2(n-1)) \\
 = & \text{Mul} \times (1/3 \times n(n-1)(n+7) \\
 & - 2(n-1)) \\
 = & \text{Mul} \times (1/3 \times (n-1)(n^2+7n-6)) \\
 = & (1/3 \times n^3 + 2n^2 - 13/3 \times n + 2) \text{Mul}
 \end{aligned}$$

【0129】

従って、方程式求解部全体の計算量は、

$$\begin{aligned}
 & ((1/3 \times n^3 + 2n^2 - 13/3 \times n + 2) + (4n-5) + 1/2 \times \\
 & n(n+1)) \times \text{Mul} + \text{Inv} \\
 = & (1/3 \times n^3 + 5/2 \times n^2 + 1/6 \times n - 3) \times \text{Mul} + \text{Inv}
 \end{aligned}$$

Inv = 40Mul、n = 5と仮定したとき、計算量は、142Mulである。

2. 2 その他の変形例

(1) p を素数、 $q = p^n$ 、 n を正の整数、有限体 $GF(p)$ の拡大体 $GF(q)$ 上の楕円曲線を E 、楕円曲線 E のベースポイントを G とし、楕円曲線 E 上の離散対数問題を安全性の根拠として利用して、安全性を確保しながら通信する暗号通信システム、デジタル署名通信システム及び誤り訂正通信システムなどの通信システムにおいて、安全性の確保に際して、拡大体 $GF(q)$ 上の元の逆元を算出する逆元演算を行う場合に、上記に説明した方程式求解部及び逆元演算装置を適用するようにしてもよい。前記暗号通信システムの一例は、インターネット上での E-mail システムにおいて、メッセージを暗号化して送受信する場合である。また、デジタル署名通信システムの一例は、電子決済システムである。また、訂正通信システムの一例は、前記 E-mail システムにおいて、通信回線の品質の悪化等の原因により、送信メッセージの一部が欠落した場合などに、送信メッセージから欠落した部分を検出し、またさらに訂正するシステムである。

【0130】

また、前記離散対数問題を安全性の根拠としてデジタル著作物を暗号化し、DVD、半導体メモリなどの記録媒体に記録する記録装置において、また、前記暗号化デジタル著作物を復号して再生する再生装置において、暗号又は復号に際して、上記に説明した方程式求解部及び逆元演算装置を適用するようにしてもよい。

【0131】

このとき、これらの応用システムにおいて、少ない計算量で逆元演算を行うことができる。

上記の方程式求解部及び逆元演算装置は、例えば、携帯電話機に内蔵されるファームウェア、パソコンに装着される回路基盤として実装されうる。

(2) 上記の実施の形態では、 $g^n - \beta$ の形の生成多項式を扱ったが、 n 次的一般の生成多項式

$$f(g) = \beta_n g^n + \beta_{n-1} g^{n-1} \cdots + \beta_2 g^2 + \beta_1 g + \beta$$

に対しても同様にして、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数) 上の元 x の逆元 I を算出することができる。

【0132】

生成多項式を n 次の一般の多項式 $f(\alpha)$ とし、その根を α とする。

拡大体 $GF(q)$ 上の元 x ($x = x_0 + x_1 \alpha + \dots + x_{n-1} \alpha^{n-1}$) に対して、 $(x \times \alpha^{j-1} \bmod f(\alpha))$ の α^{i-1} の係数を a_{ij} とすると、 n 元連立一次方程式は、次のように表現できる。

$$a_{11}y_0 + a_{12}y_1 + a_{13}y_2 + \dots + a_{1n}y_{n-1} = 1$$

$$a_{21}y_0 + a_{22}y_1 + a_{23}y_2 + \dots + a_{2n}y_{n-1} = 0$$

...

$$a_{n1}y_0 + a_{n2}y_1 + a_{n3}y_2 + \dots + a_{nn}y_{n-1} = 0$$

次に、上記のように n 元連立一次方程式を表現できる根拠について簡単に説明する。

【0133】

$$\begin{aligned} x \times I &= x \times y_0 + x \times y_1 \times \alpha + \dots + x \times y_{n-1} \alpha^{n-1} \\ &= 1 \bmod f(\alpha) \end{aligned}$$

である。

$$\begin{aligned} &x \times y_0 + x \times y_1 \times \alpha + \dots + x \times y_{n-1} \alpha^{n-1} \\ &= x \times y_0 + (x \times \alpha \bmod f(\alpha)) \times y_1 + \dots \\ &\quad + (x \times \alpha^{n-1} \bmod f(\alpha)) \times y_{n-1} \end{aligned}$$

であり、 α^{i-1} の係数は、

$$a_{i1} \times y_0 + a_{i2} \times y_1 + \dots + a_{in} \times y_{n-1}$$

で与えられる。

【0134】

α^{i-1} ($i > 2$) の係数は、すべて 0 であり、 α^0 ($i = 1$) の係数は 1 であるので、上記の n 元連立一次方程式が得られる。

(3) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0135】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク

、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0136】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を搬送波に載せて、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を搬送波に載せて、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(4) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0137】

【発明の効果】

以上に説明したように本発明は、有限体 $GF(p)$ (p は素数) 上の n 元連立一次方程式 $Ax = b$ (n は正の整数、 A は n 行 n 列の成分からなる係数行列、 x は n 個の成分からなる変数ベクトル、 b は n 個の成分からなる定数ベクトル) の解を求める連立方程式求解装置であって、係数行列 A と定数ベクトル b とを記憶しているパラメタ記憶手段と、前記パラメタ記憶手段から係数行列 A と定数ベクトル b とを読み出し、読み出した係数行列 A 及び定数ベクトル b を三角化変換して方程式 $Ax = b$ と同値の関係を有する n 元連立一次方程式 $Cx = d$ の係数行列 C (C は n 行 n 列の成分からなる係数行列) 及び定数ベクトル d (d は n 個の成分からなる定数ベクトル) を生成する三角化変換手段と、前記三角化変換は、係数行列 A の各対角成分を 1 に変換しない、係数行列 A の上三角行列への変換であり、生成された係数行列 C の各対角成分の有限体 $GF(p)$ 上の逆元である対角逆元を生成する対角逆元演算手段と、生成された係数行列 C と定数ベクトル d と生成された各対角逆元とを用いて、方程式 $Ax = b$ の解として、方程式 $Cx = d$ の解を求める方程式求解手段とを備える。

【0138】

この構成によると、連立方程式求解装置の計算量を削減することができる。

ここで、前記三角化変換手段は、連続する 1 個以上の変換過程を介して前記方程式 $Cx = d$ の係数行列 C 及び定数ベクトル d を生成し、前記各変換過程において、前記三角化変換手段は、変換前の n 元連立一次方程式から、変換前の n 元連立一次方程式と同値の関係を有する変換後の n 元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前の n 元連立一次方程式は、方程式 $Ax = b$ であり、最後の変換過程において、変換後の n 元連立一次方程式は、方程式 $Cx = d$ であり、前記各変換過程において、前記変換前の n 元連立一次方程式は、変換の対象となる 1 個以上の n 元一次方程式である対象方程式と、変換の軸となる n 元一次方程式である軸方程式とを含み、前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第 1 係数群と第 2 係数群とを定め、ここで、前記第 1 係数群と前記第 2 係数群とは、それぞれ軸方程式に係る 1 個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くことにより、前記対象方程式において 0 でない係数を有する最高次の変数の係数が 0 となる前記同値方程式が得られ、前記対象方程式において、0 でない係数を有する最高次の変数の係数を 0 とし、前記対象方程式において、0 でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第 1 係数群に含まれる値を乗じ、得られたそれぞれの値から前記第 2 係数群に含まれる値を引くように構成してもよい。

【0139】

この構成によると、連立方程式の係数行列の対角行列を 1 としないように、三角化変換が行える。

ここで、前記三角化変換手段は、前記各変換過程において、1 個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記三角化変換手段は、各副変換過程において、軸方程式の 0 でない係数を有する最高次の変数の係数から構成される群を第 1 係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の 0 でない係数を有する最高次の変数の係数を乗じ、得られた各値から構

成される群を第2係数群と定め、前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし、前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引くように構成してもよい。

【0140】

また、前記三角化変換手段は、前記各変換過程において、1個の係数群算出過程と、前記係数群算出過程後に1個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記係数群算出過程において、前記三角化変換手段は、軸方程式及び1個以上の対象方程式の0でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる2以上の値から構成される群を第1係数群と定め、前記第1係数群に含まれる値であって、軸方程式の0でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた1個以上の値から構成される群を第2係数群と定め、前記副変換過程において、前記三角化変換手段は、前記対象方程式において、0でない係数を有する最高次の変数の係数を0とし、前記対象方程式において、0でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第1係数群に含まれる値を乗じ、得られたそれぞれの値から前記第2係数群に含まれる値を引くように構成してもよい。

【0141】

これらの構成によると、三角化変換において同値の関係を有する方程式を得ることができる。

ここで、係数行列Cの対角成分を m_i ($i = 1, 2, \dots, n$)とし、対角成分 m_i のGF(p)上の対角逆元を I_i ($i = 1, 2, \dots, n$)とし、

前記対角逆元演算手段は、

【0142】

【数 28】

$$t_i = \prod_{k=1}^n m_k \text{ (} m_i \text{ を除く) mod } p$$

$$(i=1, 2, \dots, n)$$

【0143】

を算出し、

【0144】

【数 29】

$$t = \prod_{k=1}^n m_k \text{ mod } p$$

【0145】

を算出する乗算部と、 $u = 1/t \text{ mod } p$ を算出する第1逆元演算部と、対角逆元 $I_i = u \times t_i \text{ mod } p$ ($i=1, 2, \dots, n$) を算出する第2逆元演算部とを含むように構成してもよい。

また、前記乗算部は、 $s_1 = m_1 \times m_2 \text{ mod } p$ 、 $s_2 = s_1 \times m_3 \text{ mod } p$ 、 \dots 、 $s_{n-3} = s_{n-4} \times m_{n-2} \text{ mod } p$ をこの順序で算出し、次に、 $t_n = s_{n-3} \times m_{n-1} \text{ mod } p$ 、 $t_{n-1} = s_{n-3} \times m_n \text{ mod } p$ 、 $s_n = m_{n-1} \times m_n \text{ mod } p$ 、 $t_{n-2} = s_{n-4} \times s_n \text{ mod } p$ 、 $s_{n-1} = m_{n-2} \times s_n \text{ mod } p$ 、 $t_{n-3} = s_{n-5} \times s_{n-1} \text{ mod } p$ 、 $s_{n-2} = m_{n-3} \times s_{n-1} \text{ mod } p$ 、 $t_{n-4} = s_{n-6} \times s_{n-2} \text{ mod } p$ 、 \dots 、 $s_5 = m_4 \times s_6 \text{ mod } p$ 、 $t_3 = s_1 \times s_5 \text{ mod } p$ 、 $s_4 = m_3 \times s_5 \text{ mod } p$ 、 $t_2 = m_1 \times s_4 \text{ mod } p$ 、 $t_1 = m_2 \times s_4 \text{ mod } p$ をこの順序で算出し、次に、正の整数の集合 $\{1, 2, \dots, n\}$ から選択された1個の値 j について、 $t = t_j \times m_j$ を算出するように構成してもよい。

【0146】

これらの構成によると、対角逆元を算出する演算プロセス内において、逆元演算の回数を削減することができる。

こうして計算量を削減することができ、高速な暗号方式や署名方式を可能にする有限体上の連立方程式求解装置を提供することができ、その実用的価値は大きい。

【0147】

また、本発明は、有限体 $GF(p)$ (p は素数) の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数) の元 x の逆元 I を演算する逆元演算装置であって、元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay = B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、上記の連立方程式求解装置であって、 n 元連立一次方程式 $Ay = B$ の解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備える。

【0148】

この構成によると、計算量の少ない逆元演算装置を提供することができる。

また、本発明は、有限体 $GF(p)$ (p は素数) の拡大体 $GF(q)$ ($q = p^n$ 、 n は正の整数) の上の楕円曲線を E 、楕円曲線 E のベースポイントを G とし、楕円曲線 E 上の離散対数問題を安全性の根拠として利用して安全性を確保する通信を行い、安全性の確保に際して拡大体 $GF(q)$ 上の元 x の逆元 I を算出する通信システムであって、元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay = B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、上記の連立方程式求解装置であって、 n 元連立一次方程式 $Ay = B$ の解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備える。

【0149】

この構成によると、有限体上の逆元演算において計算量の少ない通信システムを提供することができる。

また、本発明は、有限体 $GF(p)$ (p は素数) の拡大体 $GF(q)$ ($q =$

p^n 、 n は正の整数)の上の楕円曲線を E 、楕円曲線 E のベースポイントを G とし、楕円曲線 E 上の離散対数問題を安全性の根拠として暗号化されたデジタル著作物を記録している記録媒体から暗号化デジタル著作物を読み出して復号し、復号に際して拡大体 $GF(q)$ 上の元 x の逆元 I を算出する記録媒体再生装置であって、元 x と拡大体 $GF(p)$ 上の多項式の係数とを用いて、 n 元連立一次方程式 $Ay=B$ の係数行列 A 及び定数ベクトル B を生成する方程式生成手段と、上記の連立方程式求解装置であって、 n 元連立一次方程式 $Ay=B$ の解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元 I を算出する逆元算出手段とを備えることを特徴とする。

【0150】

この構成によると、有限体上の逆元演算において計算量の少ない記録媒体再生装置を提供することができる。

【図面の簡単な説明】

【図1】

本発明の1の実施の形態としての逆元演算装置100の構成を示すブロック図である。

【図2】

逆元演算装置100の全体の動作を示すフローチャートである。

【図3】

逆元演算装置100の方程式の係数行列の三角化変換の動作を示すフローチャートである。

【図4】

逆元演算装置100の対角成分の逆元演算の動作を示すフローチャートである。

【図5】

逆元演算装置100の方程式の演算の動作を示すフローチャートである。

【図6】

方程式変換部102を適用する具体例である。

【図7】

方程式変換部 1 0 2 a による係数行列の三角化変換の動作を示すフローチャートである。

【図 8】

変形例としての方程式変換部 1 0 2 a を適用する具体例である。

【図 9】

従来のエルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。

【図 1 0】

従来の係数行列の三角化変換の動作を示すフローチャートである。

【図 1 1】

従来の方程式変換を適用する具体例である。

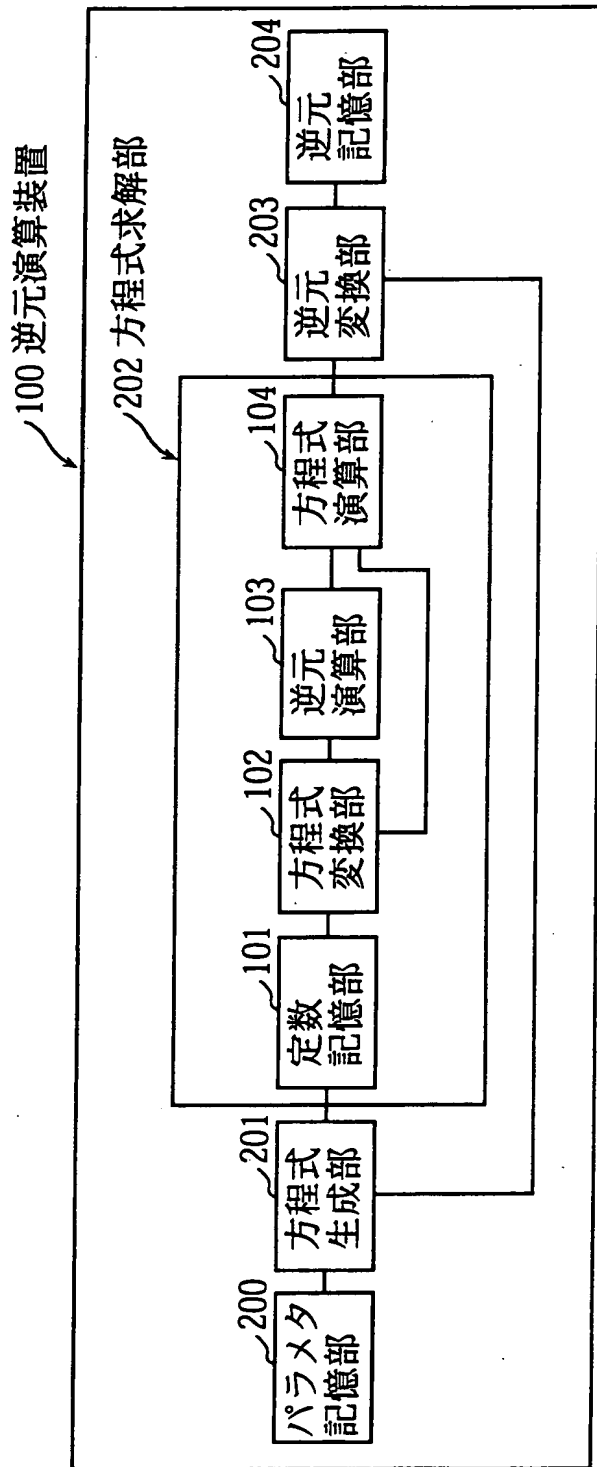
【符号の説明】

1 0 0	逆元演算装置
1 0 1	定数記憶部
1 0 2	方程式変換部
1 0 2 a	方程式変換部
1 0 3	逆元演算部
1 0 4	方程式演算部
2 0 0	パラメタ記憶部
2 0 1	方程式生成部
2 0 2	方程式求解部
2 0 3	逆元変換部
2 0 4	逆元記憶部

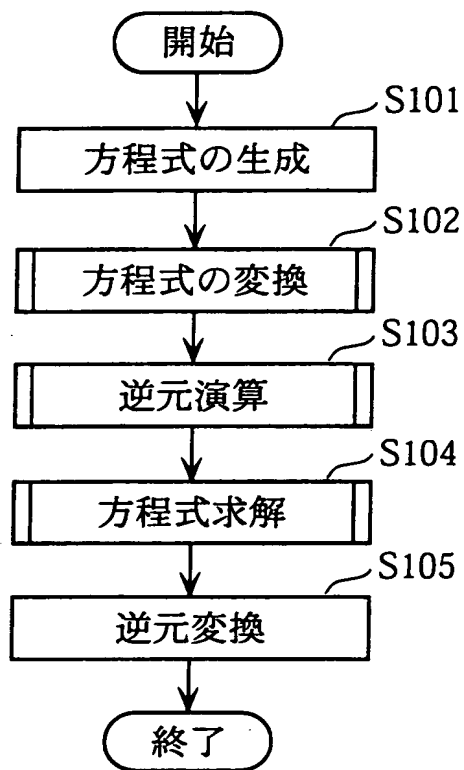
【書類名】

図面

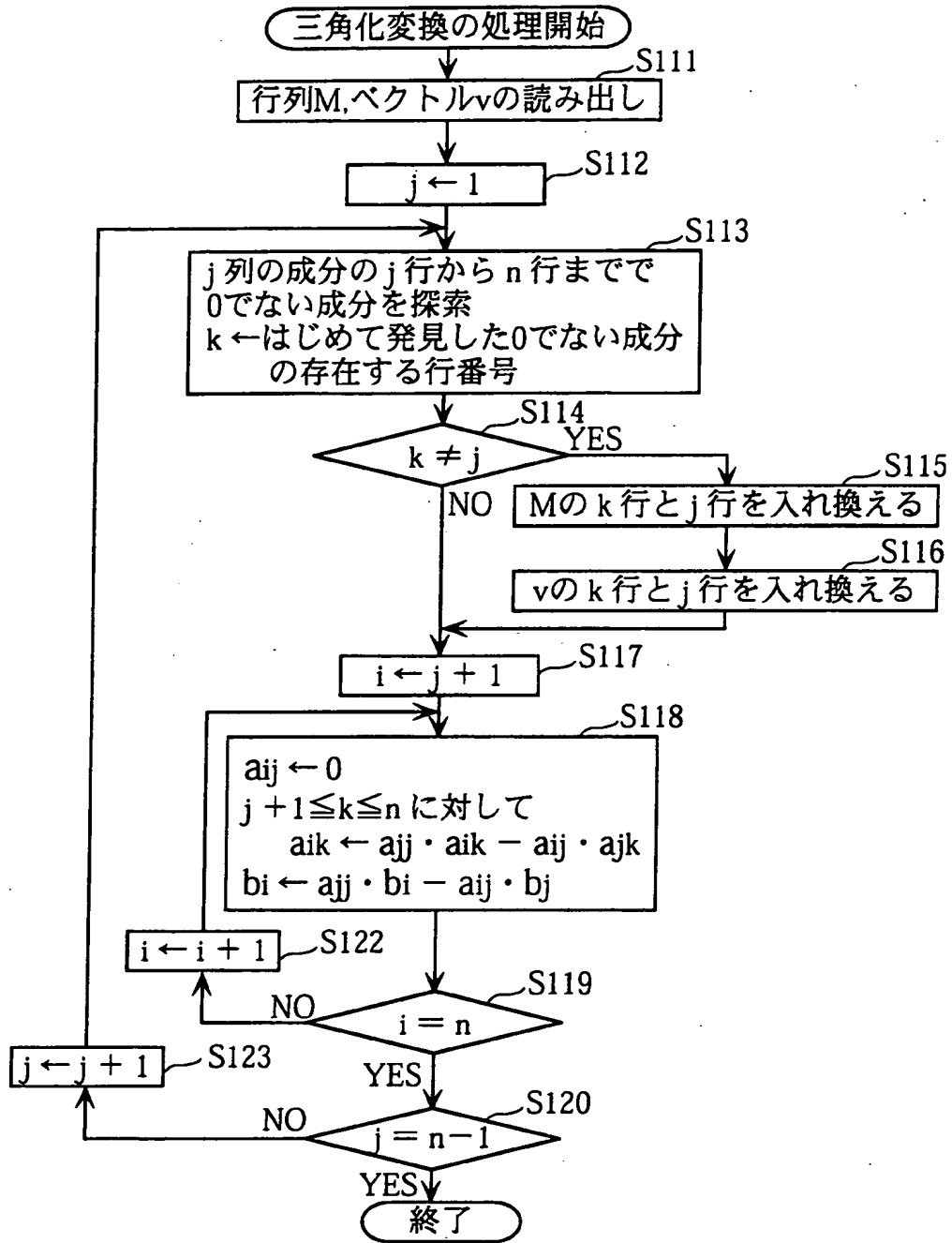
【図 1】



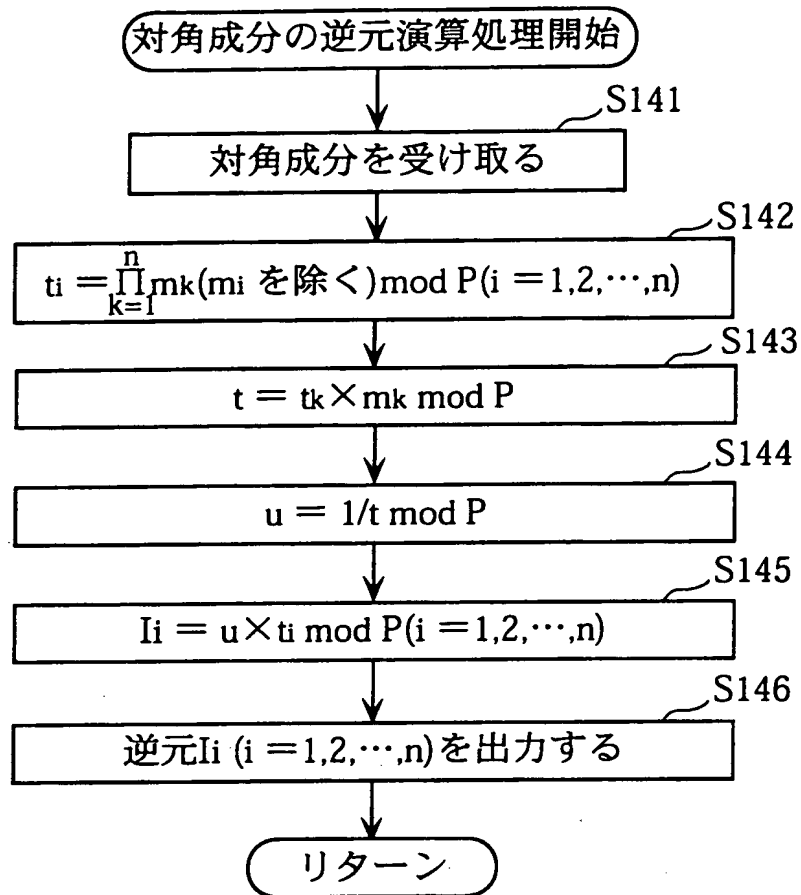
【図 2】



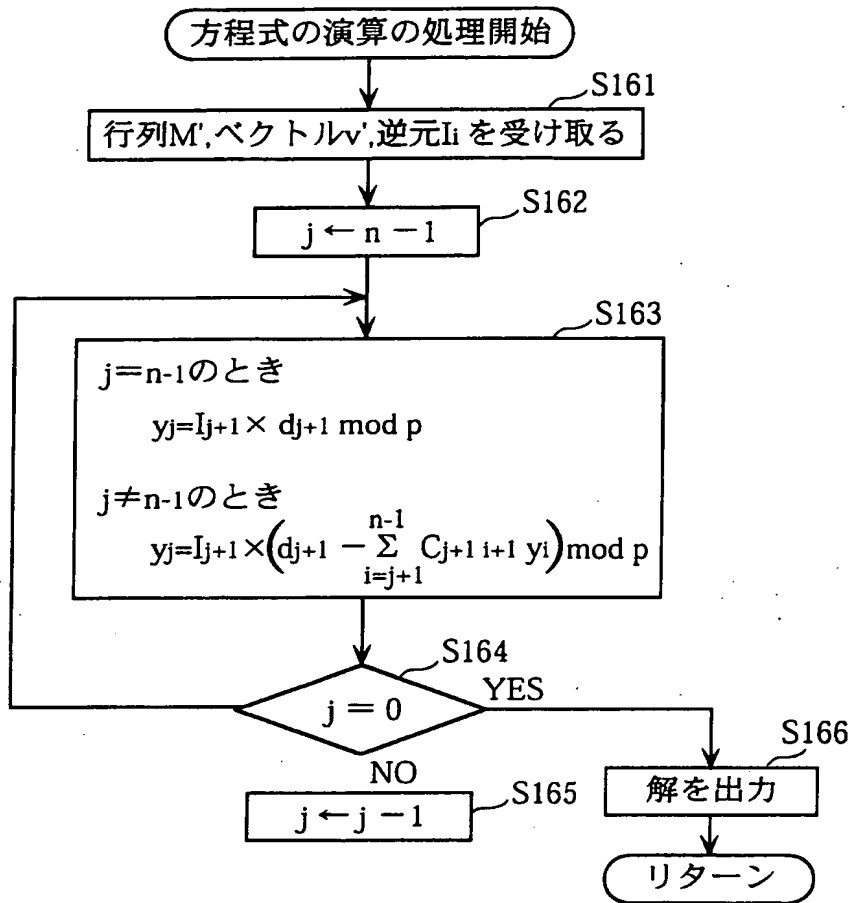
【図 3】



【図 4】



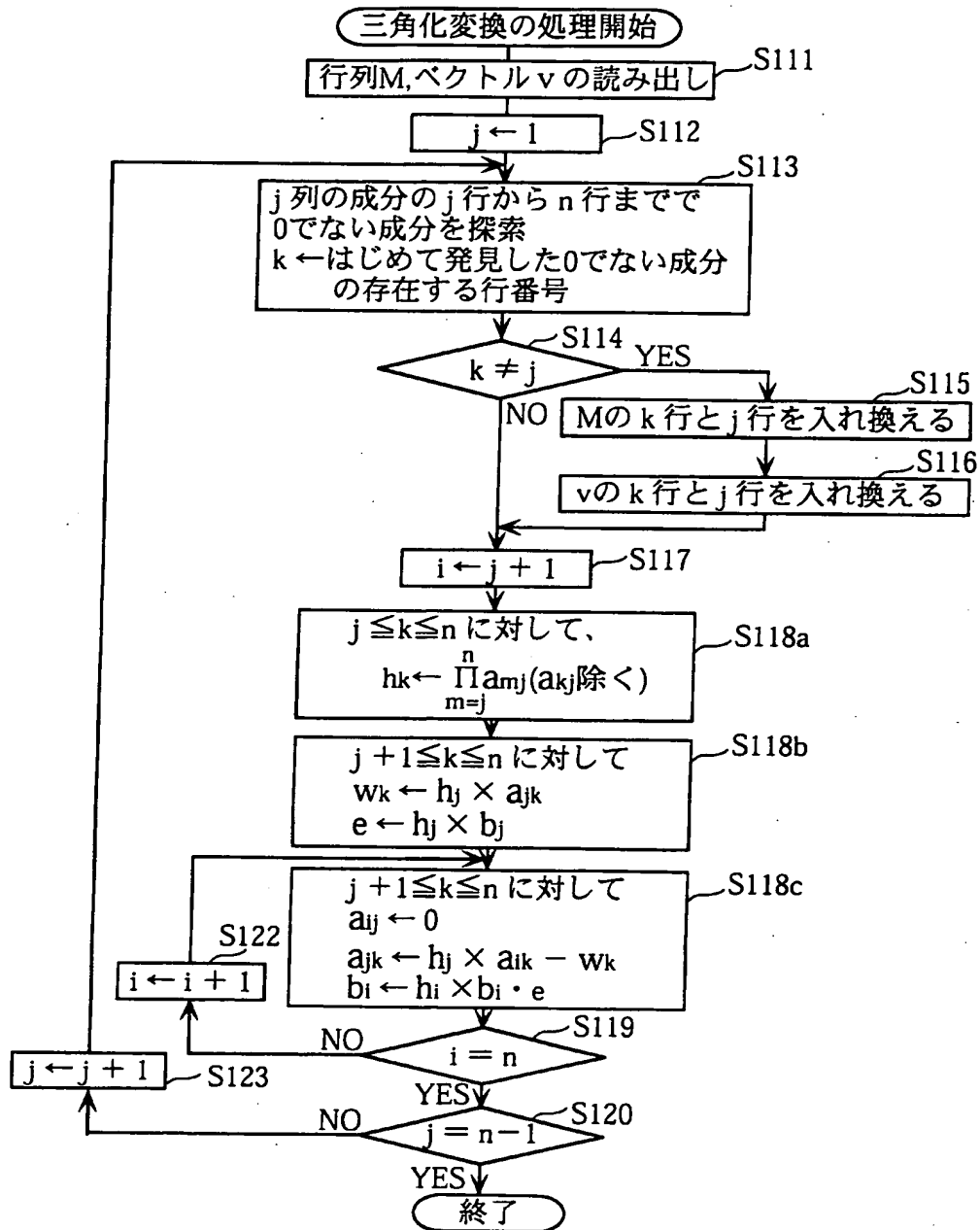
【図 5】



【図 6】

$$\begin{array}{l}
 \text{(a)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
 \text{(b)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ \boxed{0} & 6 & 29 & 14 & 9 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ \boxed{12} \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
 \text{(c)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ \boxed{0} & 15 & 3 & 5 & 14 \\ \boxed{0} & 29 & 5 & 3 & 29 \\ \boxed{0} & 9 & 29 & 15 & 6 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ \boxed{25} \\ \boxed{2} \\ \boxed{26} \end{pmatrix} \\
 \text{(d)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & \boxed{0} & 17 & 6 & 11 \\ 0 & \boxed{0} & 26 & 15 & 6 \\ 0 & \boxed{0} & 6 & 26 & 17 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ \boxed{1} \\ \boxed{5} \\ \boxed{17} \end{pmatrix} \\
 \text{(e)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & 0 & 17 & 6 & 11 \\ 0 & 0 & \boxed{0} & 6 & 2 \\ 0 & 0 & \boxed{0} & 3 & 6 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ 1 \\ \boxed{28} \\ \boxed{4} \end{pmatrix} \\
 \text{(f)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & 0 & 17 & 6 & 11 \\ 0 & 0 & 0 & 6 & 2 \\ 0 & 0 & 0 & \boxed{0} & 30 \end{pmatrix} \times \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ 1 \\ 28 \\ \boxed{2} \end{pmatrix}
 \end{array}$$

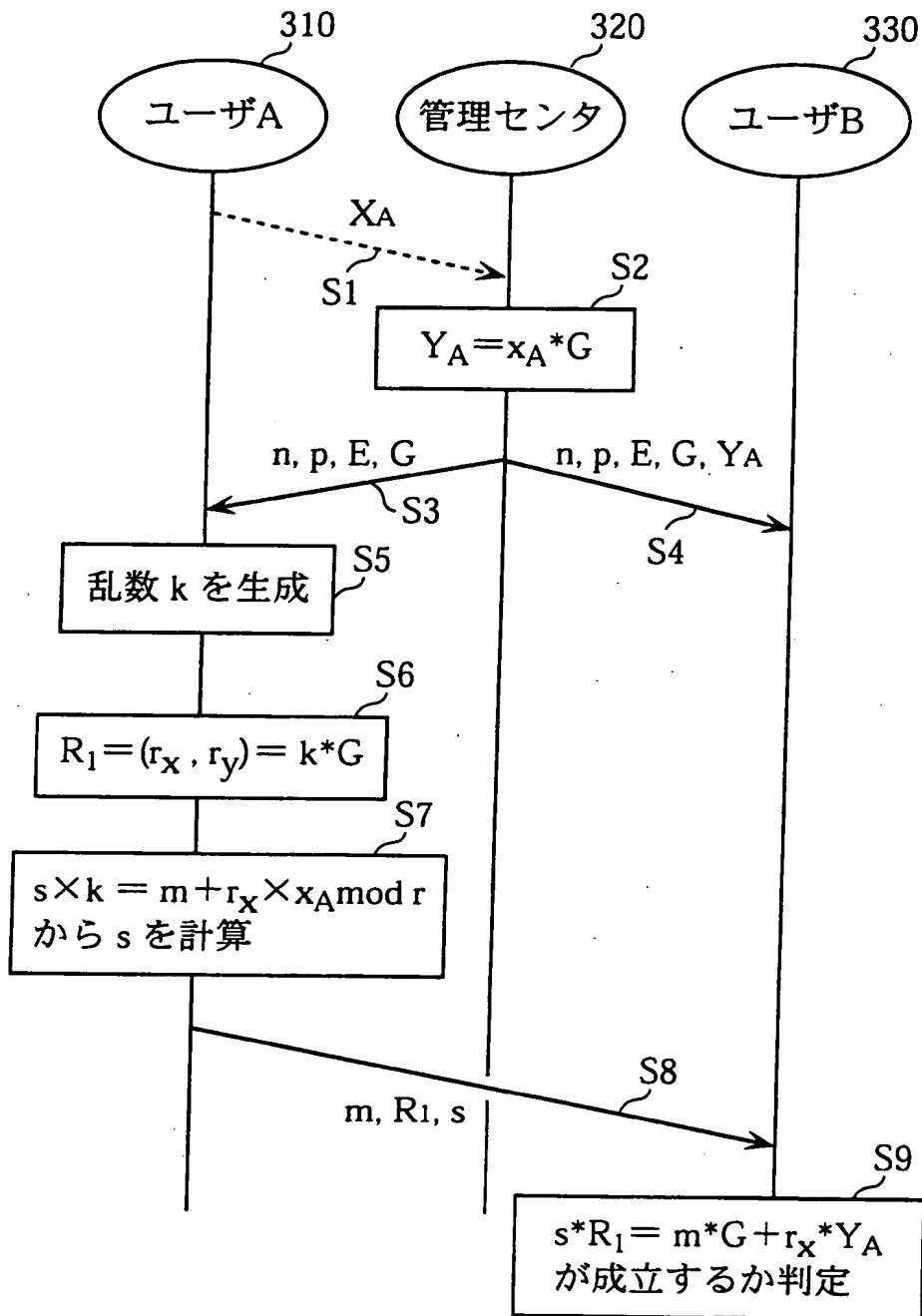
【図 7】



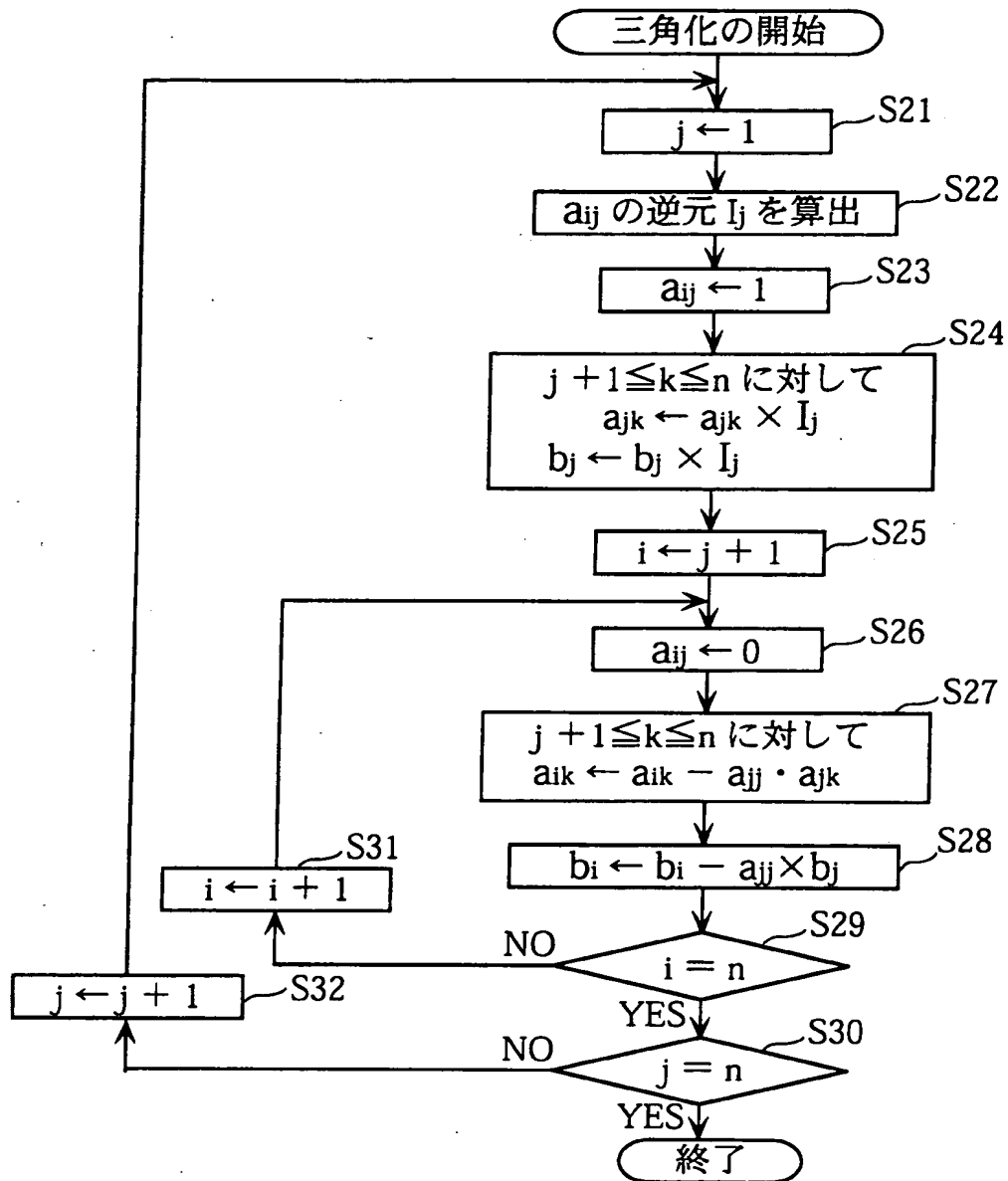
【図 8】

$$\begin{array}{lcl}
 \text{(a)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}^{501} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}^{502} \\
 \text{(b)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ \boxed{0} & \boxed{12} & \boxed{27} & \boxed{28} & \boxed{18} \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}^{511} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ \boxed{24} \\ 0 \\ 0 \\ 0 \end{pmatrix}^{512} \\
 \text{(c)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ \boxed{0} & 2 & 19 & 11 & 6 \\ \boxed{0} & 7 & 29 & 5 & 7 \\ \boxed{0} & 25 & 22 & 21 & 27 \end{pmatrix}^{521} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ 24 \\ \boxed{24} \\ \boxed{24} \\ \boxed{24} \end{pmatrix}^{522} \\
 \text{(d)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & \boxed{0} & 8 & 1 & 7 \\ 0 & \boxed{0} & 14 & 20 & 8 \\ 0 & \boxed{0} & 12 & 21 & 3 \end{pmatrix}^{531} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ 24 \\ \boxed{26} \\ \boxed{17} \\ \boxed{3} \end{pmatrix}^{532} \\
 \text{(e)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & 0 & 8 & 1 & 7 \\ 0 & 0 & \boxed{0} & 16 & 26 \\ 0 & 0 & \boxed{0} & 14 & 28 \end{pmatrix}^{541} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ 24 \\ 26 \\ \boxed{23} \\ \boxed{29} \end{pmatrix}^{542} \\
 \text{(f)} & \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & 0 & 8 & 1 & 7 \\ 0 & 0 & 0 & 16 & 26 \\ 0 & 0 & 0 & \boxed{0} & 22 \end{pmatrix}^{551} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} & = \begin{pmatrix} 1 \\ 24 \\ 26 \\ 23 \\ \boxed{18} \end{pmatrix}^{552}
 \end{array}$$

【図 9】



【図10】



【図 11】

$$\begin{array}{ll}
 \text{(a)} \quad \begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \text{(f)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 1 & 4 & 28 \\ 0 & 0 & 27 & 12 & 11 \\ 0 & 0 & 11 & 27 & 26 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 11 \\ 4 \\ 26 \end{pmatrix} \\
 \text{(b)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \text{(g)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 1 & 4 & 28 \\ 0 & 0 & 0 & 28 & 30 \\ 0 & 0 & 0 & 14 & 28 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 11 \\ 17 \\ 29 \end{pmatrix} \\
 \text{(c)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 4 & 9 & 30 & 6 \\ 0 & 10 & 2 & 24 & 30 \\ 0 & 9 & 24 & 2 & 9 \\ 0 & 6 & 9 & 10 & 4 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 8 \\ 27 \\ 22 \\ 7 \end{pmatrix} & \text{(h)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 1 & 4 & 28 \\ 0 & 0 & 0 & 1 & 21 \\ 0 & 0 & 0 & 14 & 28 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 11 \\ 15 \\ 29 \end{pmatrix} \\
 \text{(d)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 10 & 2 & 24 & 30 \\ 0 & 9 & 24 & 2 & 9 \\ 0 & 6 & 9 & 10 & 4 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 27 \\ 22 \\ 7 \end{pmatrix} & \text{(i)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 1 & 4 & 28 \\ 0 & 0 & 0 & 1 & 21 \\ 0 & 0 & 0 & 0 & 13 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 11 \\ 15 \\ 5 \end{pmatrix} \\
 \text{(e)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 26 & 11 & 15 \\ 0 & 0 & 27 & 12 & 11 \\ 0 & 0 & 11 & 27 & 26 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 7 \\ 4 \\ 26 \end{pmatrix} & \text{(j)} \quad \begin{pmatrix} 1 & 17 & 18 & 8 & 15 \\ 0 & 1 & 10 & 23 & 17 \\ 0 & 0 & 1 & 4 & 28 \\ 0 & 0 & 0 & 1 & 21 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 2 \\ 11 \\ 15 \\ 29 \end{pmatrix}
 \end{array}$$

【書類名】 要約書

【要約】

【課題】 有限体上の連立方程式の求解法において、計算量を削減することができる有限体上の連立方程式求解装置を提供する。

【解決手段】 方程式変換部 102 は、行列 M 及びベクトル v を三角化変換して、 n 元連立一次方程式 $Mx = v$ と同値の関係を有する方程式 $M'x = v'$ の行列 M' 及びベクトル v' を生成し、前記三角化変換は、行列 M の各対角成分が 1 に変換されないよう、行列 M を上三角行列に変換し、逆元演算部 103 は、行列 M' の対角成分の逆元を演算し、方程式演算部 104 は、対角成分の逆元と M' と v' とを用いて方程式 $M'x = v'$ の解を算出し、逆元変換部 203 は、解に基づいて有限体 $GF(p)$ の拡大体 $GF(q)$ 上の元の逆元 I を演算する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社